The ACA and You

A HANDBOOK FOR THE MEMBERS OF
THE AMERICAN CRYPTOGRAM ASSOCIATION

WELCOME!

It is a great pleasure to greet you as a new member of the American Cryptogram Association. Draw up a chair and take your place at our round table to participate in the various activities of your organization. We are a strictly volunteer organization and expect members to help.

You should have received a copy of the ACA membership directory when you joined; find a member living near you who is willing to talk, or write to a member who may live across town, across the state, across the country, or even in another country. Many members have email addresses and that has become a good way for many to contact each other. Fellow members can often answer your questions, or you may enjoy a solving session together, exchanging tips and tricks.

Please feel free to write, email, or phone any of the Officers or Editors about any questions you may have or any problems on which you may be stuck. The mailbox and the door are always open.

Make yourself at home – and Good Solving!

Preface

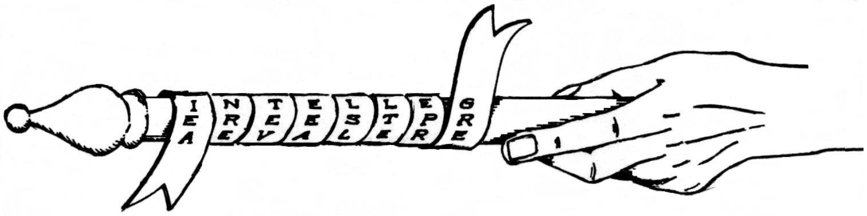
This publication is not meant to be a how-to-solve book. However, over the years there are many members who have successfully used it toward that purpose. It is intended as an introduction to the ACA: history, terminology, and descriptions and guidelines for encrypting the various types of ciphers used in *The Cryptogram*. It is a handbook, and to expect more is to expect too much.

The 2005 edition differed from the 1988 edition in corrections to and re-ordering of the text, the addition of details of the Monome-Dinome cipher and Headlines, updated reading lists, and activities. A more comprehensive Table of Contents should make finding what you are looking for easier. Care has been taken not to split the description of a particular cipher across page boundaries. Feel free to use the extra space for notes or doodles. At the back are appendices containing Morse code symbols, Vigenère, Variant, Beaufort and Porta Tables and various Syllabary tables.

Subsequent editions contain additions, corrections, and minor re-ordering of the text to the 2005 edition. Information about hyphenation usage in ciphertext is now found in Chapter 7. This seemed to be a more fitting placement of the information and allowed space for the Sudoku encryption guidelines are in Chapter 8. Chapter 10 has been expanded to include more terms and jargon.

In 2016 more corrections and additions were made and details about the CONDI, Syllabary, and Numbered Key Cipher have been included as well as including tables for the Syllabary in English, French, German, Italian, Latin, and Spanish in the appendices.

To the volunteers, known and unknown, who assisted with the production of this publication, thank you.



WHAT IS THE SCYTALE?

Scytale (fr. Gr. skytale). Spartan message in (transposition) cipher. The meaning of the Greek term is stick, staff, club, or pole.

The scytale is the official symbol of the ACA and is the center of the ACA emblem found on the front cover. The word is Greek and is pronounced sitaly, (as in Italy) or perhaps as skitaly – but never as sky-tail.

Originally it described a rod or baton carried as a badge of office. It is still used by military officers today. Used as an early enciphering device, a parchment was wrapped spirally around it, and the text was written-in lengthwise. A similar rod at the receiving end permitted correct decipherment. The word scytale is now used for the message as well as the medium.

A reference to a scytale is found in an Ode by Pindar in 468 B.C.; and an early English reference is in North's translation of Plutarch's "Life of Lysander", dated 1595. North did not bother to translate the term. The Romans used the word "scytala", changing only the suffix to make the word behave according to the rules of Latin grammar.

Above is an artist's impression of how it might work in practice. We've added a Latin tag reading INTELLEGERE EST PRAEVALERE. To understand is to succeed. As with all good mottoes, it reads as well backwards as forwards.

(For a more detailed discussion of the history of the scytale, and how to pronounce it, please refer to **DENDAI**'s article in *The Cryptogram* JA75 et seq.)

Table of Contents

Chapter 1

A Brief History of The American Cryptogram Association

The American Cryptogram Association was organized originally to place the "cryptogram" on an equivalent basis with chess, thus contributing to the happiness of mankind. It has grown to encompass many phases of cryptography, using both pencils and paper and computers.

During the 1920s, *Detective Fiction Weekly* had a feature on cryptography by M. E. Ohaver. Dr. C. B. Warner and some friends were attracted by the technical aspects of this as a hobby and joined to form the American Cryptogram Association on September 1, 1929. The ACA was at first concerned only with what we now call mono-alphabetic substitution ciphers, termed by them "The Aristocrat of Puzzles".

Meanwhile, in Burton, Ohio, George Lamb ran the "Secret Corner" in the local newspaper. He read Ohaver's column and was also a member of the National Puzzler's League (NPL). The ACA inherited the idea of using noms-de-plume, noms, as a means of bringing equality – or at least anonymity – to their cipher-solving from the NPL. Lamb chose **DAMONOMAD** as his nom and became known as **DAMON**. He too was concentrating on Aristocrats. With the demand for his column increasing, he and Warner agreed to publish a magazine which would be the official journal of the ACA. It was to be named *The Cryptogram*. The first issue appeared in February, 1932. The ACA now has members all over the world, and *The Cryptogram* has grown to a 32-page bimonthly journal with six major departments.

In 1933, "The Master Puzzler" was published and contained the name of Helen Fouché Gaines under the nom of **PICCOLA**. Her major interests were in ciphers – various systems of disguising text aside from the Simple Substitution. Her first article appeared in *The Cryptogram* in December 1933, and was followed by the opening of the "Cipher Exchange" in that issue. In August 1933 the “Foreign Cryptogram Department”, now known as “Xenocrypts”, appeared in *The Cryptogram*.

In 1936, interest having grown in ciphers and methods of breaking them, it was suggested that the ACA publish a textbook. The contents would be taken from the "Round Robin" lessons that had been a major method of spreading information and practice among members with additional material from foreign sources and hard-to-find books. With help from many volunteers, *Elementary Cryptanalysis* (*Elcy*) appeared for the first time in 1939, under the editorship of Helen Fouché Gaines. The book was also dedicated to George Lamb, who died before it appeared in print. **PICCOLA** died soon after. *Elcy* was the first book of its kind to appear in English and was reprinted by Dover in 1956 under the title *Cryptanalysis*. It remains a standard text to this day. The ACA has since published many other booklets on specialized subjects. Each was produced by volunteers among our members.

In 1982 a regular "Computer Column" was started. In deference to those who do not possess computers, only hints and suggestions for enciphering and deciphering but not fully developed programs are published in this column. In 1986, a Computer Supplement was published; it contained more information on computer activities. Lack of involvement from interested members led to the dissolution of this publication. At the present time, archived copies of the computer supplement can be found at http://www.cryptogram.org/computer_supplements/

Cryptography has been more than merely an entertainment for the enjoyment of ingenuity. It engages the mind fully and can provide a healthy period of work for those unable to do much else. George Lamb was confined to a wheelchair, and the world of cryptography opened its content as well as its friendships to him. So captivating are the efforts required in grappling with a problem, it can become a harmless addiction – a passion.

A member reminded us once that it's a nice hobby in that it can be enjoyed with no more equipment than a pencil, an eraser, paper, and little expense beyond postage and a membership in the ACA which includes a subscription to *The Cryptogram*.

The ACA is a non-profit organization devoted to the dissemination of cryptographic knowledge. There are few limits on membership. Officers receive no reward for service other than the joy of promoting cryptography.

Cryptographers are diversified in every way. Hardly a trade or profession has missed representation among us. Age is not a factor; we have had members under 10 and over 90. Formal education seems totally unrelated to the curious talent. The use of noms brings a degree of anonymity to the members; only cryptography counts. We are banded together in an organization which represents everyone with these aims: to gain the most from a study of cryptograms, to form worthwhile friendships, and to pass on the knowledge we have been able to add to the Art.

Once a year members and friends, experts and novices, gather at the ACA Convention. Many meet for the first time, although they may be old friends by mail or email. New enthusiasm is generated for the hobby as mutual help is given and experience is shared.

Chapter 2

Reading List and Resources

Kahn, David. *The Codebreakers*. New York. Macmillan, 1967.

A monumental - 1164 pages - history of codes and ciphers from ancient Greece to the present day. Good descriptions of the mechanics of cryptanalysis, with emphasis on the people involved. Also available in paperback from Signet (brutally abridged).

Note: A revised edition was published in November 1996.

Gaines, Helen Fouché. *Cryptanalysis*. New York. Dover, 1956.

Originally published before the war, this is the amateur cryptanalyst's bible. Clear, concise descriptions of many ciphers and how to attack them.

Sinkov, Abraham. *Elementary Cryptanalysis A Mathematical Approach*. Washington DC: The Mathematical Association of America, 1966.

This book contains a well-written description of several ciphers. More limited range than Gaines, but the treatment is deeper, with extremely good analysis of the mathematics involved. The third edition contains some BASIC programs for computer analysis.

Friedman, William F., and Lambros D. Callimahos. *Military Cryptanalytics*. Part 1 Vol. 1. Aegean Park Press,1985.

Advanced solving methods for simple substitution, polygraphic substitution such as Playfair, and irregular substitution such as monome-dinome.

Friedman, William F., and Lambros D. Callimahos. *Military Cryptanalytics*. Part 1 Vol. 2. Aegean Park Press,1985.

Tables of frequency data for English and other languages, and challenge problems supporting MC Part I Volume I.

Callimahos, Lambros D., and William F. Friedman. *Military Cryptanalytics*. Part 2 Vol. 1. Aegean Park Press, 1985.

Advanced solving methods for repeating-key systems such as Vigenère and Quagmires, symmetry of position, Progressive Key, and advanced polyalphabetic systems.

Callimahos, Lambros D., and William F. Friedman. *Military Cryptanalytics*. Part 2 Vol. 2. Aegean Park Press, 1985.

Introduction to traffic analysis, tables and problems supporting MC Part II Volume I, and the extremely interesting and educational Zendian Problem.

With the demise of Aegean Park Press, Military Cryptanalytics seems to be out of print. Amazon.com lists copies when available, some at reasonable prices. Copies of one volume or another appear occasionally on *abebooks.com with high prices. At this writing there is no copy on eBay, but it's worth checking now and then. Libraries may be another resource for books that were published by Aegean Park Press.*

Gleason, Norma. *Cryptograms and Spygrams.* New York. Dover, 1981.

Good introduction to the simpler cons.

REYNARD's children's series *Secret Code Breaker*.
http://www.secretcodebreaker.com

(Reviews of books and software are a regular feature in *The Cryptogram*.)

Specialty Publisher

The Aegean Park Press no longer exists. You need to check for used copies.

Specialty Journals

Cryptologia, a quarterly journal devoted to Cryptography, is published by Taylor & Francis Group. www.tandfonline.com

The ENIGMA is the monthly magazine of the National Puzzlers' League.
http://www.puzzlers.org

ACA Publications

In addition to *The Cryptogram*, the ACA publishes various booklets of special interest to members:

Solving Simple Substitution Ciphers - by Frances A. Harris (**S. TUCK**).

An introduction to Aristocrats, Patristocrats, and Xenocrypt substitution! Monoalphabetic substitutions are covered in thorough detail, from the Caesar substitution, through the first principles to the use of pattern words. The text includes statistics for French, German and Italian. 42pp, 9x6. (1959)

Practical Cryptanalysis - five volumes by W. M. Bowers (**ZEMBIE**) and William G. Bryan (**B. NATURAL**)

This series was intended as a follow-up for *Elementary Cryptanalysis* published in 1939, to bring the cryptanalytic methods up to date and to include additional ciphers not found in the earlier book. The treatment and examples are particularly matched to the ciphers found in *The Cryptogram*. (1967). Each volume is 9x6.

Volume 1 - Digraphic Substitution. Playfair and Four Square ciphers are dealt with at length, starting with identification and peculiarities and leading into sample problems and solutions. The Seriated Playfair is explained, and a test for the period demonstrated. (46 pp.).

Volume 2 - The Bifid Cipher. A description of the cipher and how to encipher it is followed by the Three Square Technique, finding the period, and solving the Three Squares. The peculiarities of the Even Period lead into Conjugated Matrix Bifids, and the continuous encipherment cycle. (48 pp.)

Volume 3 - The Trifid Cipher. A brief biography of the mysterious F. Delastelle, the inventor of both the Bifid and the Trifid ciphers, is followed by a description of the cipher and its peculiarities, keyword recovery, “naturals”, locating tips, use of patterns and repeats, etc. (54 pp.)

Volume 4 - Substitution and Transposition Ciphers. This covers 22 of the “Cipher Exchange” ciphers not discussed in the other volumes in this series. A must for anyone attempting these ciphers, the booklet gives a brief description of each cipher and a worked analysis of the solution. (45 pp.)

Volume 5 - Periodic Ciphers: Miscellaneous. This volume discusses the general problem of finding the period, and then deals in detail with the Vigenères, Portax and Nihilist Substitution. A digression on alphabet recovery is followed by Quagmires, Auto -, Running -, and Interrupted-Key ciphers, the Tri-Square, Fractionated Morse, Seriated Playfair, and Homophonic ciphers, 17 in all. (45 pp.)

3 Ways to Solve Cryptograms - This booklet consists of three sections each by a different author: “Cryptometry Simplified”, by Henry C. Wiltbank (**NYPHO**); “The Graphic Position Chart”, by Lewis S. Sutcliff (**RED E. ERASER**); “The Care and Feeding of Cryptograms”, by Lisle J. Maxson (**FLUKE**). All are aimed at the beginner cryptanalyst tackling substitution ciphers (Aristocrats and Patristocrats).

> The first section describes how to make a Contact Chart, and how to interpret it. The second shows what may be learned by noting the relative positions of letters, which start words and which end words, and so forth. The last section suggests vowel and consonant hunting as a fast means to a solution and includes hints on those Special Cases designed to trip up unwary solvers. Published in 1963, but still very valid. (14 pp., 11x8)

An Approach to Cryptarithms - by Frederick D. Lynch (**FIDDLE**), introduces the reader to the subject with some fundamentals of notation, and a description of keyed and unkeyed cryptarithms. The Negation Square is introduced as a means of keeping track of which numbers are known and which are not. Theorems of Triplication in Threes, Casting Out Nines, etc. and 28 “short-cut” theorems follow. The book finishes with discussions on Double Key Cryptarithms, The Duodecimals, and some tables of higher-base numbers. Although this is an older publication, a great deal of fundamental information is packed into its pages. (24 pp., 9x6)

Solving Cryptarithms- This 28 page booklet by Jack Winter (**CROTALUS**) was published in 1984 and is an expansion of his series of articles in *The Cryptogram* JF73-JF74. It explains notation, analyses a classical Cryptarithm, discusses Searching for Zeroes and Nines, Multiplication, Divisions, Roots and Other Base problems. The use of Multiplicative Structures is given in detail. The author shows how brute force methods can be used for “toughies”. The book concludes with some useful Appendices, including how to compute square and cube roots, and Tables of Decimal, Undecimal and Duodecimal functions. (28 pp., 9x6)

Novice Notes - by Gerhard D Linz (**LEDGE**) covers many of the ciphers found in the Cipher Exchange, higher numbered Xenocrypts, and the Analyst Corner. Each chapter discusses how to set up a particular cipher type and then discusses the solving process. There are ciphers at the end of each chapter for further practice. (148 pp., 11x8.5)

Xenocrypt Handbook - compiled and edited by William G. Sutton (**PHOENIX**), this book contains data and articles from a variety of sources. Those Language Data Sheets that have appeared in past issues of *The Cryptogram* form the nucleus of the handbook, and are all represented along with pertinent articles. Aids to construction and guidelines are also included, as are aids to solving with specific examples for a few cryptograms in common languages. You will also find help and statistics for the determination of cryptograms in unknown languages. (96 pp., various sizes)

Manual For Cryptanalysis of the Columnar Double Transposition Cipher (A Study of Cryptanalysis) - Joseph B. Courville (**GUNG HO**) In World War II double incomplete columnar transposition was used by several governments. Although it was sometimes solved by the "general transposition attack" which required multiple anagramming of ciphers in the same key and of the same length, these were not always available to the analyst. **GUNG HO**'s course teaches a pencil-and-paper attack on the more general case, including ciphers whose lengths are close but not identical. (91 pp., 11x8)

ACA Publications on CD-ROM 2009 - contains all ACA publications listed above and *The ACA and You* (2010).

***The Cryptogram* on CD-ROM 1932-2009** is given to each member. This CD-ROM contains all copies of *The Cryptogram* and *The ACA and You* (2010).

For current prices, additions, and other FOR SALE items, please refer to a current issue of *The Cryptogram*.

ACA Website
The website for the ACA is http://www.cryptogram.org. Information about the ACA: dues, errata from cons in *Cm*, information about ACA events, information about events that may be of interest to members, resources that have been posted, etc., can be found on the website.

Chapter 3

How to Read *The Cryptogram*

The Cryptogram, like any technical journal, uses a variety of terms and expressions (jargon) that you may find a little difficult to follow at first. Apart from editorial text and articles, you will want to know how the actual cipher problems are organized.

If the front cover has a decorative pattern (an "Ornamental"), there will be a message hidden in it. Try to find repeated shapes that might represent letters of the alphabet - then solve the cipher!

The back cover carries the solutions ("Sols") for the problems given in the issue published four months previous.

Inside the magazine, the various classes of ciphers have a section or department. Within each department, the ciphers are printed in approximate order of increasing difficulty. Each problem is identified by a letter and number, e.g. E-6, the cipher type (e.g. "Ragbaby"), and a title which may give an idea of the subject matter. The name or "Nom" of the encipherer is given last on the title line. A clue or crib word is often given in parentheses using lowercase for a plaintext crib, and UPPERCASE for a Caesar substitution crib (each letter is moved N places in the alphabet). There may be additional information such as the number of characters, or some statistics on the cipher, to help you transcribe it correctly and/or do the mechanical analysis.

"Aristocrats" are simple substitution ciphers. Each plaintext letter is replaced by a different ciphertext letter not equal to itself. "Patristocrats" are the same except that the word spacings are removed to make them more difficult to decipher.

"Cipher Exchange" ciphers are in a variety of formats; the type is usually given, because there is generally not enough text to find the type by statistical methods. Details of the ciphers in current use in the "Cipher Exchange" are given later in this booklet.

"Xenocrypts" are foreign language ciphers. It is not usually necessary to be fluent in that language to find a solution to a Xenocrypt. It is possible to recover the keyword which may be in English.

"Cryptarithms" are arithmetical problems in which numbers are replaced by letters. The "number of words" given with each puzzle refers to the keyword or keywords used to develop the original number/letter equivalence. A statement such as "0-9" gives the order in which to specify the answer, e.g. in this case, the regular decimal set 0, 1, 2 . . . 9.

The "Analyst Corner" contains more difficult ciphers. Sometimes the type is not given, there is no crib, the ciphertext is in an unusual format, or some other ACA rule is broken. Because statistical analysis is often required to solve these ciphers, they may be longer than those in the rest of the magazine.

For many members, the hunt is more fun than the kill, but for those who would like to compare their ability with others, a "Solvers List" is published in each issue. (See Chapter 6 for instructions on how to submit solutions to this column.)

Chapter 4

How to Solve a Problem in *The Cryptogram*

A typical issue of *The Cryptogram* contains 13-14 pages of cipher puzzles, or "cons" (constructions). No information is included on how to solve these problems; all you are given is the type of cipher, a hint as to the subject of the con, and often a crib (tip) which is a piece of the plaintext. If you are new to decipherment, you will probably need some help on how to proceed. Here are a few notes; more details can be found in the literature.

Enciphered Tips

In real world cryptography one would have an indication of the subject matter, and probably a wealth of ciphertext. Space limits us, so we try to compensate by giving titles and tips. Enciphered tips are those that are optional for solving. They are enciphered so that those who want a greater challenge can ignore them. For those who need the help, the tips are recovered by running down (or up) the alphabet, as tips are always enciphered in a Caesar cipher. The Caesar shift is not normally more than six in either direction.

```
EXAMPLE 1:                           EXAMPLE 2:
Enciphered tip:  Z L Z H I B           Enciphered tip:  U Q E K G V A
                 A M A I J C                            T P D J F U Z
                 B N B J K D           Plain tip:       S O C I E T Y
Plain tip:       C O C K L E
```

Here the Caesar shifts are -3 and +2. Unless the tip is simply giving the period of the cipher, it is ALWAYS found somewhere in the message. Enciphered tips are always in UPPERCASE, and plain tips are in lowercase.

Keyword Recovery

A keyword is an easily remembered group of words, letters, or numbers originally, and still used, by correspondents who wish to use known methods of encipherment and still maintain secrecy. Many ciphers use a keyword to generate ciphertext alphabets to scramble the order of the message before, during or after encipherment. Recovery of the keyword offers an alternative or parallel path to solution alongside direct recovery of the plaintext. As the plaintext is revealed, so is the keyword, and guessing a letter in one may give a letter in the other that might aid solution.

Keywords are discussed in more detail in Chapter 8.

General Properties of Letters

A large vocabulary is helpful, but even more useful is a knowledge of the habits of letters and their relationships to each other in English (or the language of the message). A typical frequency table for normal English is:

E	T	AO	NIR	SH	LD	CUPF	MWY	BGV	KQXJZ	
13	9	8	7	6	4	3	2	1	-	total: 100

The high-frequency letters ETAONIRSH make up about 70% of plain text. Vowels AEIOU and Y make up about 40% of the text. Consonants LNRST make up about 35% of the text. The low frequency letters occupy less than 3% of the text but are important because of their rarity and because adjacent letters (contacts) are more likely to be vowels than consonants. Some cons are manipulated, some heavily, to change these standard frequencies.

We will now take a look at the various letters in more detail. Do not be intimidated by these statistics! Refer to them as you solve; be aware that they exist; and over time you will find they become second nature to you.

Vowels

1-letter words : A, I; O occasionally.
2-letter words : begin with A, I, O, U; end with E, O, Y.
Doubles : O, E often double; A, U, I, Y rarely double.
Digraphs A : follows E, O (EA is most frequent); reverses with I, U, Y.
E : precedes A; follows O; reverses with I,U, Y.
I : follows U, Y; reverses with A, E, O.
O : precedes A, U; reverses with I, Y.
U : follows O; precedes I; reverses with A, E.
Y : follows U; precedes I; reverses with A, E, O.

Common Positions:
A : initial and 2nd from end.
E : 2nd and final, also scattered throughout.
I : 3rd from end.
O : 2nd and final.
U : initial and 2nd from end.
Y : final.

Vowel-Consonant Digraphs

ER-RE is the most frequent reversed digraph.

A:	follows H;	precedes N,T,S;	reverses with R.
E:	follows H;	precedes S,D;	reverses with R,T.
I:	follows H,R,D;	precedes N;	reverses with T,S.
O:	follows T,S,H;	precedes N;	reverses with R,L.
U:	follows S,T,F;	precedes N;	reverses with P,B.
Y:	follows L,R,T,N;	precedes S.	

High-Frequency Consonants HLNRST

H: likes 1st, 2nd, last position; precedes vowels; follows W, S, C, T. Note TH and GHT.

L: likes 2nd, next-to-last; prefers vowel contacts; follows P, C, B; precedes P, D; doubles at 3-4 in 6-letter words; before final S, Y in 5-letter words; in last position in 4-letter words.

N: likes last and next-to-last position; follows vowels; precedes D, T, G, S, C.

R: likes 2nd and next-to-last (thus looks like a vowel, BUT it reverses freely with vowels); follows B, P, T; precedes T, S; doubles freely; often reverses with T (a common consonant reversal); seldom follows S.

S: likes last (very strongly), 1st and third position; doubles freely at middle and last positions; follows vowels and D, T, R, N; precedes vowels and T, H, P, C, M; reverses often with T.

T: likes 1st, last and next-to-last (also scatters); doubles freely; follows vowels and B, C, F, L, N, P, R, S, X; precedes vowels and H, R.

The following two consonants (with E, S, T, N, R, Y) end most English words:

D: likes 1st and last position; prefers vowel contacts; doubles freely when followed by L; follows L, N, R; precedes R, W, L.

G: likes last (strongly), sometimes 1st, 3rd from last and next-to-last; doubles freely when followed by L; follows vowels and D, R, N; precedes vowels and H, R, L.

Other Consonants

(These, with T, O, S, begin most English words).

B follows vowels; precedes vowels, L, R; doubles when followed by L.
C follows vowels, S, N; precedes vowels, H, T, L, R, K; doubles.
F follows vowels; precedes vowels, T, R; doubles within and last.
J usually initial only, precedes O, U; never doubles.
M follows vowels, S, R; precedes vowels, P; doubles within.
P follows vowels, R, L, M, S; precedes vowels, R, L, T; doubles freely.
V follows vowels, L, R; precedes vowels.
W follows vowels, D, S, T; precedes vowels, H, R.

Low-Frequency Consonants

K likes first position followed by vowel or N; last position preceded by N, R, C, L; otherwise contacts vowels.
Q likes 1st, 2nd, 3rd positions; normally followed by U; preceded by E, O, N, S, C.
X follows vowels and N; precedes vowels and C, H, P, T.
Z contacts vowels on both sides normally. (NB: UK uses "S" for USA "Z" in many instances.)

The Index of Coincidence

The Index of Coincidence (IC) is a powerful test to help the analyst decide whether a set of ciphertext has been encrypted with the same alphabet. It measures the roughness of the frequencies: that is, if the letter frequencies are about equal, the frequencies are smooth. Natural language tends to have a rough frequency distribution. To calculate the IC, take a frequency count of the individual letters. For each letter, multiply the frequency by the frequency minus one, then add them all together. Divide the sum by N * (N-1), where N is the number of letters in the sample. The result is the IC. For example, the frequencies of the first sentence in this paragraph are:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
8	2	7	5	22	3	0	10	8	0	0	4	1	6	5	5	0	4	6	14	1	0	3	2	2	0

The numerator is 8*7 + 2*1 + 7*6 + 5*4 + 22*21 + 3*2 + 0*(-1) + 10*9 + 8*7 + 0*(-1) + 0*(-1) + 4*3 + 1*0 + 6*5 + 5*4 + 5*4 + 0*(-1) + 4*3 + 6*5 + 14*13 + 1*0 + 0*(-1) + 3*2 + 2*1 + 2*1 + 0*(-1) = 1050, and the denominator is 118 * 117 = 13,806, so the IC is 0.0761. The expected IC for English is about 0.066, but in practice, because of statistical variations in the sample, anything over 0.055 is quite likely to be from a single alphabet. If the value is near 0.0385, the expected value for random text, the sample is almost certainly not from a single alphabet.

Different languages will have different expected IC's.

Solving Aristocrats

An Aristocrat is a simple substitution cipher with word divisions. No letter stands for itself.

Check the title first, and think of any word that might appear in the text. Look for short common words and pattern words. Make a frequency count to determine likely letter equivalencies. Look for 3 and 4-letter words, especially those containing TH. Look for common endings and beginnings.

Look for these short words: an, in, is, it, on, to, and, are, has, his, her, not, see, the, was, why, you, from, into, once, have, that, than, this, there, these, those.

Look for these word beginnings: an, at, be, de, dr, en, in, no, pre, pro, re, se, th, un.

Look for these word endings: ance, ant, ate, (a)ble, ded, ed, en, er, ere, es, ese, ess, est, ful, ght, ine, ing, ion, is, ist, ive, ll, lly, ment, ous, rst, ses, sts, tion.

Computer solution often involves the use of large word lists to provide word-matches, which by trial and error can then lead to a solution.

Solving Patristocrats

A Patristocrat is a simple substitution cipher without word divisions. No letter stands for itself.

Tips will suggest THE, THAT, ING, TION, OR, etc. or pattern words. A frequency count is usually needed to establish the basis for these. Proceed as for Aristocrats, looking for frequent digraphs, reversals, and letter patterns.

Computer solution usually starts with a program to locate the tip accurately in the ciphertext, after which dictionary look-up methods can be used to obtain a solution.

Solving Cryptarithms

A Cryptarithm is an arithmetical puzzle in which letters have been substituted for numbers. One letter represents one and only one number. Leading zeros are suppressed. Cryptarithms always use all digits of the key.

If a keyword or phrase is used, it will contain the same number of letters as the base of the numbering system, i.e., ten letters for a decimal system. The order of the letters in the keyword is indicated by ‘0-9', ‘1-0', ‘9-0', or ‘0-1' (for decimal problems). For higher-base systems, use A=10 decimal, B=11 decimal, and so on. The key may not make sense at all (No word).

To save space, problems are given in line-by-line form:

Example: Long Division. (One word; 1-0).
SORN / DIE = DS; - NMH = DRDN; - AHHM = AOD

Set up to solve:

```
           D S
       -------
D I E) S O R N
       N M H
       -------
       D R D N
       A H H M
       -------
         A O D
```

Take each section of the calculation in turn dealing with it as a simple addition. Look for left-hand digits; if single, they are probably 1. Look for columns containing two identical letters, try to place the zero. If a keyword is expected, be sure to fill in the equivalencies as you go.

More complex arithmetic, such as square roots, etc. should be reduced to a combination of additions to ease the solution.

The arithmetic manipulation lends itself to computer solution, although the challenge, as ever, is to find the short cuts used by the human brain or even better ones.

Solving Xenocrypts

A Xenocrypt may be any of the regular cipher types, but using a foreign language. It is usually not necessary to know the language to solve the ciphers, especially when tips are given. However, such things as small dictionaries or word lists, beginner's books, and the familiarity gained by previous attempts can be very useful.

Xenocrypts are attacked in the same way as problems in English, but using, of course, frequency tables and other data for the language in question. Additional data can be found in the literature; frequency tables for some languages are given below. Other references can be found in *The Cryptogram*, *Elcy*, and *Xenocrypt Handbook*.

Frequency Tables		**References**
English:	ETAONIRSHLDCUPFMWYBGVKQXJZ	
Dutch:	ENIATORDLSGKHVUWBJMPZCFYXQ	*Xeno Handbook*
Esperanto:	AIEONLRSTKJUDMPVBGFCZH	*Xeno Handbook*
French:	EANRSITUOLDCMPVBFGHQJZXY	MA86, *Elcy*
German:	ENIRSADTUGHOLBMCWFKVZPJQXY	MA89, *Elcy*
Interlingua:	EAILNOSTRUDCMPVGBFHXQJWYZK	MJ75
Italian:	EAIOLNRTSCDMPUVGZFBHQ	MJ86, *Elcy*
Latin:	IEUTAMSNRODLVCPQBFGXHJKWYZ	ND50
Portuguese:	AEORSINDMTUCLPQVFGHBJZX	*Xeno Handbook*
Spanish:	EAOSRNIDLCTUMPGYBQVHFZ	JF86, *Elcy*
Swedish:	AENRTSIOMGKLDVFBCHPUYJXQWZ	JA81

Note that these figures are statistical averages; thus the orders in *Elcy* are somewhat different from those in *The Cryptogram* and *Xeno Handbook* references.

Tips often give the identity of letters appearing only once, singletons, or not at all. Letters not appearing in the plaintext alphabet are marked with an asterisk.

The Cipher Exchange

This department of *The Cryptogram* contains a selection of ciphers which do not use simple substitution. Some 60 ciphers are in current use by the ACA, and these are detailed in Chapter 9. Methods of solution are found in the literature and are continually being improved, particularly with the application of computers. Exchanging ideas with other member may also help.

The Analyst Corner

These ciphers are considered somewhat harder and may break the "rules" for the cipher in some way, such as by the omission of a tip. The ciphers in this department may be longer than those in the “Cipher Exchange” to facilitate statistical analysis. A generous title or short narrative to "set the stage" is sometimes included.

Ornamentals

Ornamentals are pictorial ciphers, often found as front cover designs for *The Cryptogram* (See Steganography). The ciphers are usually Aristocrats or Patristocrats, but don’t rule out other cipher types. An ornamental should be treated as any Unknown. The challenge is to determine how the artist has hidden the message in the pattern, and then to solve it. Look for a typical "cell" that could represent a letter. Checking the dimensions of the figure may give a clue for there are likely to be 75-100 characters hidden in it.

Specials and Challenges

These are ciphers that the Editors consider more difficult than normal (such as a Patristocrat without plaintext "e"s), or examples of new types introduced in articles. Because of the nature of these ciphers, they are not included in the requirements for a complete (*) solution in the Solvers List, although they do count in the total solved.

Chapter 5

How to Use a Computer to Solve Ciphers

You may have ideas of using a computer to solve the ciphers shown in *The Cryptogram*. In many instances, this is very practicable – at least to assist in some of the clerk-work, if not to obtain a complete solution. There are even programs available for those who have computers, but no ability or desire to do their own programming. In these cases, the computer is used as a tool just like a pencil.

Because the computer must be programmed for a particular set of circumstances, there will always be a possibility that a manual encipherment will have a twist that is outside the range of the particular program. You should not therefore expect a 100% success rate. A study of why a cipher cannot be solved may lead to a better program. This is one of the challenges of using a computer.

Some ciphers lend themselves to a blend of human thought and machine trials to achieve a successful solution. The Aristocrat is an example. Programs are available which will replace a chosen letter in all its occurrences in the text, saving a great deal of paper and pencil work. Other types of cipher will yield to "brute force" trials, in which every possible combination is tried by the computer until a valid answer is obtained. Examples of this type are Caesar ciphers, some Cryptarithmetic puzzles, and the Homophonic. A human would rarely wish to use such a method, and part of the computer challenge is to see whether a short-cut can be programmed.

The computer can be very helpful in placing tips at the correct places in ciphertexts, providing an entry for cryptanalysis. If a tip is not available, there are programs that will run letter frequency counts, distributions, digram and trigram frequencies, indices of coincidence, etc., which not only assist with the cryptanalysis, but may enable the type of cipher to be determined (if unknown) and possibly the original language as well.

The computer naturally lends itself to the solution of ciphers produced by mechanical or computer means. Some of the famous machines of WWII, such as the Enigma, can be duplicated quite simply on small home computers. However, as these ciphers are usually outside the range of paper and pencil solution, they are not normally considered in *The Cryptogram*.

The computer will, of course, do a very fast job of encipherment, and in some cases a suitable enciphering program will lead to the design of a better deciphering algorithm.

It is not usually vital that the computer program run at maximum possible speed. An answer in half an hour, or a trial running all night, is not unreasonable, so many of the published programs deliberately use BASIC in order to be compatible with the largest number of machines (and the largest number of computer users). For the same reason, it is not necessary to have the latest, biggest, or fastest computer; much good work is done with machines that are now obsolete compared to modern operating systems and large applications. Even a 10-year-old computer is likely to have enough disk and memory to be able to deal with a 300,000-entry word list, and to be powerful enough to handle some brute force attacks and to support a faster language than BASIC. The size of the programs is often quite small. Of course, if you wish to hold an 80,000 word list in memory to help with pattern word searches, you will need a large machine; and, if you wish to try a brute force technique, you may wish to use a faster language than BASIC.

The Computer Column appeared in *The Cryptogram* from 1982-2013.

Chapter 6

How to Submit Your Solutions for Credit

You are encouraged to send in your solutions (sols) of the ciphers published in *The Cryptogram* to the Solution Editor. The first five words or so of recovered plaintext and/or the recovered keyword are sufficient to show proof of a solution. Unless explicitly requested, keywords, however, are not required to claim credit.

Solutions are due at the Solution Editor's desk on the first day of the FOURTH MONTH following publication. For example, solutions for the January-February issue are due on or before May 1. For reference, the due dates are given at the top of the Solvers List, as is the address to which solutions should be sent. All solutions for one issue should be submitted together on the same sheet of paper. At the top of your submission, you should include a summary line giving your nom, the issue, the number of ciphers solved in each department, the total number claimed for the issue, and the resulting Year-To-Date total. The summary provides a check point to help the Sols Editor avoid common data entry errors, overlooked solutions, etc.

Solutions may also be submitted by email to <acasols@cryptogram.org>. Please use ordinary text within the e-mail (NO attachments, NO word processor formats or formatting) with one solution per line. Include a summary line at the top of the submission with NOM, issue, column and special totals, total for the issue and YTD total.

```
JA2002   AA PP CC XX EE SS Issue YTD
MY NOM   23 14 10  6 15  3    71 312
```

Late updates obviously make more work for the Sols Editor.

Each issue of *The Cryptogram* contains a Solvers List for the third issue previous, a table of Solvers List Statistics, and the solutions for the issue two issues previous.

The department abbreviations (AA, PP, etc.) as described below are suggested. The Specials department (SS) includes all problems identified with the “-Sp” mnemonic (such as C-Sp-1 or E-Sp), those in the Analyst Corner, and any other non-regular ciphers designated as “submit for credit”, Ornamentals, etc. An asterisk may be used in place of a number when credit is claimed for solving all regular ciphers in a department.

AA for Aristocrats,
PP for Patristocrats,
CC for Cryptarithms,
XX for Xenocrypts,
EE for Cipher Exchange,
SS for Specials (including Analyst Corner)

The figures in each column show the number of successful solutions in each class for that issue of *The Cryptogram*. The last column is the running Year-To-Date total for the calendar year. The maximum score possible is shown at the end together with the number of persons submitting solutions. An asterisk in a column means all ciphers in that particular department have been solved. An asterisk behind the name or nom means that all departments have been completed, except Specials. The latter are not required for a "complete" (asterisk), since they are unusual. The Table of Statistics will show you how many solvers solved each problem, giving you an idea of which ones were found to be easy and which difficult. [In each department, the editor attempts to rank the problems from the easiest to the most difficult.]

It is possible that you may get stuck on a cipher, and require help. Feel free to write to the Department Editor for a further hint. Whether you then enter the solution for credit is entirely up to you. The scores in the Solvers List reflect your own personal pleasure and standards; you will not be asked whether yours is a joint effort, or whether you used dictionaries or computers, or other aids to help. The scores are not meant to be any more competitive than you want them to be. While it is true that you may gain more satisfaction from solving a tough cipher than from solving one with a generous tip, each contributes its own solving pleasure. Your score is your record of your progress. Not everyone has the skill, time, or energy to scale the heights.

You may also claim credit for problems submitted and published in *The Cryptogram*. In this case, just add the solution to the rest of your solutions being claimed for the issue in which your problem is printed.

An annual Honor Roll is published showing those with 300 or more solutions for the year, and Certificates of Achievement are given after each 1000 solutions. As there about 100 cons in a typical issue, it may take you some time to get your first certificate!

The submitted solutions also give us some idea of who is doing what. They help all the editors. They also add up over the years. If you dislike some, or cannot spend your limited time on those requiring extra effort, there is no shame in a blank or a single entry in a department.

Chapter 7

How to Encipher a Problem for *The Cryptogram*

The Cryptogram depends on you for problems published for the pleasure of all. Make a note of interesting plaintext as you read. Polish your language skills and gain new insights by enciphering. Then send the results to the Department Editors so others may pit their skills against your challenge!

No game is entertaining unless players are assured a square deal. Thus, to ensure justice and to maintain high standards, guidelines have been worked out over the years. All are subject to editorial judgment in individual cases. A contribution which meets the standards will always be more welcome than one which does not.

The departments give varied fare for experts and beginners. Your contribution will be tested by the Department Editor and graded for difficulty. You are encouraged to add a title and tip to your contribution. Editors may override these suggestions. However, if you have not suggested a title or tip, a suitable tip and title may or may not be added by the editor.

Please use a separate sheet of paper for each encipherment, write on one side of the paper only, and use the format employed for that cipher in *The Cryptogram*. You should show your working of the solution on a separate page. If submitted by email, please use a separate message for each con and include the type of cipher in the subject line.

We hope all members will contribute generously and regularly so the Editor's "bins" (files) will be kept full. Remember that a published "con" can be counted as a "sol".

Enciphering Guides

1. Text must make sense. Check word meanings to avoid impossibilities and contradictions. Telegraphic text, incomplete sentences without verbs, or mere lists of words are not acceptable.

2. Definite and indefinite articles may be omitted, but punctuation must be correct for Aristocrats. Numerals are to be written out in full (except for those cipher using 6x6 Polybius squares and other ciphers using digits in their alphabets, such as a 36 letter Ragbaby).

3. Misspelling, mixed cases, wrong tenses, or other grammatical errors must be avoided. Check and recheck before submitting.

4. When a ciphertext contains word divisions and occupies more than one line when printed, there can be ambiguity as to whether a word at the end of a line is complete or not. To avoid confusion use these conventions for hyphens and word breaks:

   Use the single hyphen (-) to indicate that a ciphertext word is continued on the next line. This does not indicate proper syllabic hyphenation.

   Use a double hyphen (=) to indicate that the original plaintext word is hyphenated.

   Use a repeated double hyphen (= =) to indicate a dash to separate thoughts.

5. Text worth reading should be the solver's reward. Unfair tactics reduce the value of the challenge; cleverness is the essence of a tough problem. Find what features of the cipher aid in its decipherment, and see if you can obscure these features suitably.
6. Double-check quotations to make sure they are accurate. If they are being paraphrased brutally for an Aristocrat that's one thing, but if they are intended to be literal quotes they should be quoted correctly.
7. Follow the guidelines in this book for proper lengths for ciphers. Good problems may have to be discarded because of excessive length, but don't spoil a poem or a quotation for the sake of a few letters!
8. Unfair text contains words not listed in standard dictionaries with the exception of proper nouns and popular slang. Obsolete words, reformed spellings, and foreign words are unacceptable.
9. In Xenocrypts, simple language is preferred to technical quotations. Accents are always omitted. In simple substitutions, use a keyword to aid in deciphering irregular verbs, singletons, etc. (K2s are preferred; K3s, K4s, and random alphabets must not be used). (See Chapter 8 for the types of keys.)

   Keys may be in English or in the foreign language, but should be chosen to assist the decipherment. Study what other encipherers do.
10. In Simple Substitutions, use only capital letters. No letter may stand for itself. Add an asterisk to the left of any proper noun in an Aristocrat, Keyphrase, or Ragbaby, and any Xenocrypts of these types. (In Xenos an asterisk is also used in the tip to denote a letter or group of letters that do not actually appear. That is, it may be used to denote one or more letters missing in the alphabet, the square, or in the text.)
11. In Periodics, the ciphertext should be submitted in blocks of five letters.
12. In Cryptarithms, use no base under 8 or over 16. Bases 10, 11, 12, and 16 are preferred. Root extractions are limited to square and cube roots. There must be only one possible solution to a Cryptarithm. Check, for instance, that any letters occurring once only are not in the same column.
13. Editors may choose to use the American spelling of a British word in a quotation by a British author.

The Question of Original Systems

One-time pads were used by spies and were unbreakable. Rudolf Abel's cipher was probably also unbreakable. His messages were not read until he explained the cipher, and even knowing the general system, it may still confound many people. More recently, Bruce Schneier invented a playing-card-based system called Solitaire which has so far resisted attacks.

So you have the perfect indecipherable system? Perhaps you have heard that the ACA is a proving ground for such things? Stop! While we all like a challenge, the purpose of the ACA is not to test for indecipherable systems.

For over 400 years, cryptographers have been writing seriously on the subject. Systems once thought to be unbreakable have succumbed to analysis. Without a thorough knowledge of what has been done, and of what makes a good system, the chances of inventing a useful new one are slim. Variations are endless and too often worthless.

Below is a list of guidelines for a successful military cipher. Variations for diplomatic and commercial use are minor, but in any case the ciphers are intended for heavy traffic use with difficulty of solution appropriate to the timeliness of the enciphered message. Few cryptographers are able to judge the weak spots of a system, even one that seems to meet the requirements. If you do invent a new one, let it sit for a while and "digest" in your mind while you try to find a similar system already in use, or used in the past.

Note that we already use some 60 ciphers in *The Cryptogram*. To be considered seriously, you would first have to describe your new cipher in an explanatory article. Based on this, and your own record of ability in cryptography, the system might be considered for acceptance for regular use if the reaction of the membership were favorable.

Auguste Kerckhoffs (1835-1903), was a Flemish linguist and cryptographer. The most famous dictum on his list is #9, which is commonly called “Kerckhoffs’ Law”. His criteria for a suitable military cipher are:

1. The cipher must be suitable for telegraphic transmission, with no special symbols.
2. Ciphertext should not be much longer than the plaintext for rapidity in encipherment, transmission, and legitimate decipherment.
3. Security must not depend on any limitations of plaintext.
4. Decipherment must yield unambiguous plaintext; one possible message. A few ACA ciphers do not obey this rule.
5. Necessary apparatus must be small enough to be easily carried.
6. Methods of encipherment and decipherment must be simple, requiring few operations and putting little mental strain on the operator.
7. Errors being inevitable, omission or error in a letter or group should not affect the rest of the text. Rapid and easy correction must be possible.
8. Text comparisons of several cipher messages with a fragment of plaintext, or with the text of another cipher, should not lead to a "break".
9. Kerckhoffs’ Law: The interceptor is assumed to possess all details of the system but the keyword. An unalterable system, or one with few variations, is poor. The key must be easily altered, easily remembered, easily applied, and vastly variable.

During World War II the ACA was the proud reservoir of cryptographic talent for our country. Today, paper and pencil work is still vital to our national well-being. The FBI has professional codebreakers solving ciphers much like ours, so our skills are still useful. In considering new systems for presentation to the ACA, we give more weight to the cryptanalytic interest, subjectively judged, than to adherence to any specific requirements. Experience must still back any invention, for only through solving can you come to judge the degree of interest your own invention might generate among fellow members.

Chapter 8

ACA Guidelines

Keywords

Keywords may be used in Aristocrats, Patristocrats, Cryptarithms, Xenocrypts, and in many Cipher Exchange systems. Although a key may be optional, its use is recommended not only because it is a useful aid to solution but also because it reflects the historical use of keys in these ciphers.

Four basic schemes are referred to by number, K1 to K4. The alphabet is keyed by writing an arbitrary keyword or phrase followed by the rest of the alphabet in normal order. A letter occurring more than once is omitted after the first occurrence.

e.g. CONSTELLATION becomes CONSTELAI.

Either the plaintext or the ciphertext alphabet may be shifted ("wrapped round") to avoid a plaintext letter standing for itself in simple substitutions.

Regular Alphabetic Keywords

K1 Keyword Type: plain alphabet contains a key, CIPHER alphabet is normal.

pt:	**p**	**o**	**u**	**l**	**t**	**r**	**y**	a	b	c	d	e	f	g	h	i	j	k	m	n	q	s	v	w	x	z
CT:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q

K2 Keyword Type: plain alphabet is normal, CIPHER alphabet has the key.

pt:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CT:	V	W	X	Z	**K**	**E**	**Y**	**B**	**O**	**A**	**R**	**D**	C	F	G	H	I	J	L	M	N	P	Q	S	T	U

K3 Keyword Type: Both alphabets are keyed with the same key.

pt:	**c**	**o**	**n**	**q**	**u**	**e**	**s**	**t**	a	b	d	f	g	h	i	j	k	l	m	p	r	v	w	x	y	z
CT:	H	I	J	K	L	M	P	R	V	W	X	Y	Z	**C**	**O**	**N**	**Q**	**U**	**E**	**S**	**T**	A	B	D	F	G

K4 Keyword Type: Both alphabets are keyed, using different keywords.

pt:	**s**	**h**	**o**	**p**	**t**	**a**	**l**	**k**	b	c	d	e	f	g	i	j	m	n	q	r	u	v	w	x	y	z
CT:	V	W	X	Y	Z	**J**	**U**	**P**	**I**	**T**	**E**	**R**	A	B	C	D	F	G	H	K	L	M	N	O	Q	S

5x5 Polybius Square

	1	2	3	4	5
1	E	O	B	K	S
2	X	D	C	L	U
3	T	I	F	M	V
4	R	N	G	P	W
5	A	Y	H	Q	Z

A Polybius Square is used to encipher plaintext in some ciphers. The use of row and column numbering may or may not be necessary. Since only a 25-letter alphabet can be used the I and J are combined in the same cell. In this example, the keyword EXTRAORDINARY is used in a vertical route. Other routes are possible.

For encryption, a plaintext or key letter J is replaced with I before encrypting. By convention, we use only I (not J) in ciphertext.

6x6 Polybius Square and 36-Letter Alphabets

	1	2	3	4	5	6
1	E	5	X	T	R	A
2	6	G	7	H	8	1
3	F	S	U	V	J	O
4	3	Q	Z	W	Ø	D
5	C	P	M	L	K	4
6	2	B	Y	N	9	I

When a 26-letter alphabet with 10 digits is used to encipher plaintext which includes numbers, then the digits MUST be placed immediately after their corresponding letters in the Polybius square or in the keyed/unkeyed alphabet: 1 after A, 2 after B, etc., whether they appear in the key or not.

The example at the left shows how to build a 6x6 square using a clockwise spiral with keyword = EXTRAORDINARY.

The following is an example of a 36-letter Ragbaby alphabet using the same keyword: E5XTRA1OD4I9NYB2C3F6G7H8J ØKLMPQSUVWZ.

Some ciphers which adapt to a 6x6 Polybius Square include:

6x6 Bifid
6x6 Twin bifid
6x6 Checkerboard
6x6 CM bifid
6x6 Foursquare
6x6 Nihilist substitution
6x6 Phillips
6x6 Playfair
6x6 Seriated playfair
6x6 Tri-square
6x6 Two square
36-letter alphabet Ragbaby

Length guidelines for 6x6 ciphers will be the same as their 5x5 counterparts.

Mixed Alphabetic Keyword Types

The keyed alphabets may be mixed rather than in normal sequence. The resulting keys are identified as K1M, K2M, etc. The mixing is done with a transposition block. The keyword alphabet is entered by rows, and the mixed alphabet is taken off by columns, either in left to right sequence or in alphabetical order of the top letters (a key):

```
R O M A N C E         By consecutive columns:
B D F G H I J         MA:  RBKVODLWMFPXAGQYNHSZCITEJU
K L P Q S T U
V W X Y Z             By order of top letters:
                      MA:  AGQYCITEJUMFPXNHSZODLWRBKV
```

A transposition block may also be formed leaving spaces for letters used in the key. This will yield a different set of Mixed Alphabets (MA):

```
R O M A N C E         By consecutive columns:
- B - D - F G         MA: RHVOBIPWMJQXADKYNLSZCFTEGU
H I J K L - -
- P Q - S T U         By order of top letters:
V W X Y Z             MA: ADKYCFTEGUMJQXNLSZOBIPWRHV
```

Other arrangements submitted will ordinarily be returned to the author for re-encipherment, or will be discarded. With a proper choice of keyword, these systems have been found sufficient for a wide range of difficulty of keyword recovery. When keywords are used as an adjunct of plaintext recovery, these systems give enough play of possibilities. Rarely, an improperly keyed problem will be printed with a key designation, or it may be labeled "Variant", as in "K2V". This is used if the alphabet is split around the keyword, (for example, A B C K E Y D F G H I L ... Z)

Decimation

Given the recovered K3 alphabet:

X V O G M Z F H Q S T B A R N D K Y P W E I U L J C,

decimation allows the solver to recover the keyword used to form the key alphabet. This process is used when trying to recover the keyword in the Headlines puzzles.

```
 1: XVOGMZFHQSTBARNDKYPWEIULJC
 3: XGFSADPIJVMHTRKWUCOZQBNYEL
 5: XZTDECMSNWJGQRPLOHAYUVFBKI
 7: XHNIOSKLMBPCFREVQDUGTYJZAW
 9: XSPVTWOBEGAIMRUZNLFDJHKCQY
11: XBUHPGNCTIFYORJSEZKVALQWMD
15: XDMWQLAVKZESJROYFITCNGPHUB
17: XYQCKHJDFLNZURMIAGEBOWTVPS
19: XWAZJYTGUDQVERFCPBMLKSOINH
21: XIKBFVUYAHOLPRQGJWNSMCEDTZ
23: XLEYNBQZOCUWKRTHMVJIPDASFG
25: XCJLUIEWPYKDNRABTSQHFZMGOV
```

That is, the first decimation at offset 1 is the original alphabet. The next is at offset 3, taking every third letter and wrapping when you get to the end: XvoGmzFhqStbA and so on. Only the offsets relatively prime to 26 are used, because otherwise the sequence repeats. Then you look carefully at each line to see which one might be composed of all vertical slices of the key table. It turns out to be offset 3:

```
X GFS ADP IJV MHT RKW UCOZ QBNY EL
```

The original mixed key alphabet is

```
Q U A G M I R E
B C D F H J K L
N O P S T V W X
Y Z
```

Standard Features of Ciphers

Aristocrats, Patristocrats, and Xenocrypt Substitutions

1. Length: 75-100 letters. Pats should be 90-105, and in no case less than 85 or more than 140.
2. No more than 4 singletons (letters used only once).
3. At least 18 different letters should be used in each problem.
4. Repeated consecutive plaintext should be avoided.
5. No more than 3 proper nouns, each indicated by " * " at the left except in the case of Patristocrats.

Cryptarithms

1. Single or double keyed problems in division, multiplication, square roots and various equations are popular.
2. Additions should have no more than 3 terms plus the total.
3. Equations should have no more than 3 items.
4. Multiplications should have no more than 3 digits in the multiplier.
5. Divisions must not end in zero to be brought down as remainder unless a legitimate subtraction follows from it in the last step.
6. Problems must show all steps involved, not just components and answers.
7. Keywords MUST be complete (CRYPTAIHMS is not acceptable).
8. Several words may be used together (HOWISFRANK is acceptable).
9. Number-bases should be in the range 8-16.
10. Sudoku guidelines
    a. There must be a unique 9-letter solution or keyword in either the forward or backward direction, as indicated below, regardless of the number of words in the solution.
    b. (No word) is not a solution for a sudoku.
    c. Forward solution (27 possible locations: left to right in a row, top to bottom in a column, left to right from top to bottom in one of the nine 3x3 blocks)
    d. A backward solution, indicated by * after the number of words, (27 possible locations: right to left in a row, bottom to top in a column, right to left from bottom to top in one of the nine 3x3 blocks)
    e. Groups of 9 characters represent each row of the sudoku (top to bottom).

Cipher Exchange

Acceptable lengths for Cipher Exchange ciphers are given with each cipher in Chapter 9.

Xenocrypts

Xenocrypts use Afrikaans, Catalan, Dutch, Esperanto, French, German*, Latin, Italian, Norwegian, Portuguese, Spanish and Swedish. Other languages may be used, often as Specials.

* In German the umlauts Ä, Ö, Ü, ä, ö and ü should be transcribed as Ae, Oe, Ue, ae, oe and ue, respectively. Ciphers contain the two vowels; a dictionary shows the umlaut. Similarly the German ß is transcribed ss.

Chapter 9

The Cipher Exchange and Cipher Guidelines

The Cipher Exchange (**CE**) is that department of *The Cryptogram* that deals with ciphers which are **NOT** simple substitutions of the Aristocrat/Patristocrat variety. Here you will find the fruits of several hundred years of development of cryptography, as cryptanalysts discovered new ways to attack a cipher, and the encipherers then complicated the ciphers to compensate. Some of the ACA systems were used historically in precisely the form we use; some are simplified to highlight unique aspects of that cipher type; and some were invented by ACA members.

CE ciphers given in *The Cryptogram* are all solvable by pencil and paper methods, although computers and other mechanical aids are often used to assist. The ciphers are printed in approximate order of difficulty (as determined by experience) in *The Cryptogram*. They are listed in alphabetical order below, together with the length recommended for a suitable plaintext.

AMSCO (period times 8-12 lines deep)

The first entry may be either a digraph or a single letter. In both even and odd periods the first column and the first row always alternate.

Solvers should be aware that a null is not required when the end of the text does not fill out the digraph-single letter or single letter-digraph pattern.

Key: 41325
pt: Incomplete columnar with alternating single letters and digraphs.

4	1	3	2	5
in	c	om	p	le
t	ec	o	lu	m
na	r	wi	t	ha
l	te	r	na	t
in	g	si	n	gl
e	le	t	te	r
sa	n	dd	i	gr
a	ph	s		

CT:
CECRT EGLEN PHPLU TNANT EIOMO WIRSI TDDSI NTNAL INESA ALEMH ATGLR GR.

AUTOKEY (40-55 letters) See: **Vigenère**

This example is a Vigenère Autokey.
Find Vigenère Table in Appendix 2 or use the insert.

pt: The autokey can be used with Vigenère, Variant, Beaufort or Porta.
Key: PRIMER

```
K:  P R I M E R T H E A U T O K E Y C A N B E U S E D W I T H
pt: t h e a u t o k e y c a n b e u s e d w i t h v i g e n e
CT: I Y M M Y K H R I Y W T B L I S U E Q X M N Z Z L C M G L

K:  V I G E N E R E V A R I A N T B E A U F O R T O
pt: e r v a r i a n t b e a u f o r t o r p o r t a
CT: M M B E E M R R O B V I U S H S X O L U C I M O
```

CT:
IYMMY KHRIY WTBLI SUEQX MNZZL CMGLM MBEEM RROBV IUSHS XOLUC IMO.

BACONIAN (25-letter plaintext maximum)

A = aaaaa	E = aabaa	I/J= abaaa	N = abbaa	R = baaaa	W = babaa
B = aaaab	F = aabab	K = abaab	O = abbab	S = baaab	X = babab
C = aaaba	G = aabba	L = ababa	P = abbba	T = baaba	Y = babba
D = aaabb	H = aabbb	M = ababb	Q = abbbb	U/V= baabb	Z = babbb

Replace each plaintext letter with its Baconian equivalent.

Example 1:

```
pt:    s     u     c     c     e     s     s
     baaab baabb aaaba aaaba aabaa baaab baaab
```

The a-units and b-units are concealed; in this example the initial letter of each word indicates a or b: A-M = a, N-Z = b.

CT:

Now is a good time to attend college. School work is a good teacher and a good builder of character. Every man should be a student and learn all that there is about a subject.

Example 2:

pt:

```
  n     o     w     i     s     a     g     o     o     d     t
abbaa abbab babaa abaaa baaab aaaaa aabba abbab abbab aaabb baaba
```

For each CT letter let A-M = a, N-Z = b.

CT:

BOWED ASTER PINED JOKED THEIR BLACK HASTE ARRAY INSET CHEST SLING.

BAZERIES (150-250 letters)

pt: Simple substitution plus transposition.

First a number less than a million is chosen (say 3752). It is spelled out and used as the key in a 5x5 ciphertext Polybius square entered in left-to-right horizontal rows. A 5x5 plaintext Polybius square is used with the alphabet in normal order vertically. In the ciphertext and plaintext squares, I and J (I/J) are combined in one cell.

pt

a	f	l	q	v
b	g	m	r	w
c	h	n	s	x
d	i	o	t	y
e	k	p	u	z

CT

T	H	R	E	O
U	S	A	N	D
V	F	I	Y	W
B	C	G	K	L
M	P	Q	X	Z

The plaintext is divided into groups governed by the key numbers, in this example: 3, 7, 5, and 2. Letters within each group are reversed. The result is enciphered using the squares to match. The ciphertext is then written in 5-letter groups.

pt:
s i m/p l e s u b s/t i t u t/i o/n p l/u s t r a n s/p o s i t/i o/n

Reversed Groups (RV):
m i s/s b u s e l p/t u t i t/o i/l p n/s n a r t s u/t i s o p/o i/n

CT:
A C Y/Y U X Y M R Q/K X K C K/G C/R Q I/Y I T N K Y X/K C Y G Q/G C/I

CT: ACYYU XYMRQ KXKCK GCRQI YITNK YXKCY GQGCI.

BEAUFORT (width of period times 10-15 lines deep)

The plaintext is written into a block under the key. All letters in the first column are enciphered using the first key letter, those in the second column using the second, and so on. Using Appendix 4 to encipher the first plaintext letter **c**, look down the key column for **R** and across the plaintext (pt) row **c**. Where the **R row** and **c column** intersect, find the ciphertext **P**.

pt: C equals K minus P

Key: R E C I P R O C A L (period = 10)

pt: c e q u a l s k m i **CT:** P A M O P G W S O D
n u s p E K K T

CT: PAMOP GWSOD EKKT.

BIFID (125-150 letters) See: CM BIFID; TWIN BIFIDS

Select a period (usually 5-13). Write the plaintext in period length groups. Below each letter write its two coordinates from the 5x5 Polybius square vertically. Now read the numbers horizontally in each period group, replacing each pair of numbers with the letter it represents in the Polybius square.

For this example the period is 7. The keyword, EXTRAORDINARY, is written into the square in a clockwise spiral. The ciphertext is written in 5-letter groups. For other cases the ciphertext can be written in period-length groups.

	1	2	3	4	5
1	E	X	T	R	A
2	K	L	M	P	O
3	H	W	Z	Q	D
4	G	V	U	S	I
5	F	C	B	Y	N

pt: Odd periods are popular.

```
pt:     o d d p e r i   o d s a r e p   o p u l a r
row#:   2 3 3 2 1 1 4   2 3 4 1 1 1 2   2 2 4 2 1 1
col#:   5 5 5 4 1 4 5   5 5 4 5 4 1 4   5 4 3 2 5 4

CT: 23 32 11 45 55 41 45 23 41 11 25 54 54 14 22 42 11 54 32 54
CT: M  W  E  I  N  G  I  M  G  E  O  Y  Y  R  L  V  E  Y  W  Y
```

CT: MWEIN GIMGE OYYRL VEYWY.

CADENUS (period not over 6)

Columnar tramp using a keyword to shift the order of the columns and at the same time to shift the starting point of each column. The latter is done by attaching a letter of the alphabet (25-letter alphabet as shown with V and W in the same cell) to each row of plaintext in the block. The first column of plaintext goes into the 2nd column of the cipher block (as determined by the key) but it begins with its 22nd letter, (Y here), since the key letter (**E** here, of **EASY**) is attached to the 22nd letter of the key column. Other columns are treated similarly. The final cipher is taken off by rows from the cipher block.

pt: A severe limitation on the usefulness of the Cadenus is that every message must be a multiple of twenty-five letters long.

CT:
SYSTR ETOMT ATTLU SOATL EEESF
IYHEA SDFNM SCHBH NEUVS NPMTO
FAREN USEIE EIELT ARLME NTIEE
TOGEV ESITF AISLT NGEEU VOWUL.

K: **EASY**

pt block					CT block			
E	**A**	**S**	**Y**	Key	**A**	**E**	**S**	**Y**
2	1	3	4		1	2	3	4
a	**s**	e	v	**A**	**S**	**Y**	**S**	**T**
e	r	e	l	Z	R	E	T	O
i	m	i	**t**	**Y**	M	T	A	T
a	t	i	o	X	T	L	U	S
n	o	n	t	V/W	O	A	T	L
h	e	u	s	U	E	E	E	S
e	f	u	l	T	F	I	Y	H
n	e	**s**	s	**S**	E	A	S	D
o	f	t	h	R	F	N	M	S
e	c	a	d	Q	C	H	B	H
e	n	u	s	P	N	E	U	V
i	s	t	h	O	S	N	P	M
a	t	e	v	N	T	O	F	A
e	r	y	m	M	R	E	N	U
e	s	s	a	L	S	E	I	E
g	e	m	u	K	E	I	E	L
s	t	b	e	J	T	A	R	L
a	m	u	l	I	M	E	N	T
t	i	p	l	H	I	E	E	T
e	o	f	t	G	O	G	E	V
w	e	n	t	F	E	S	I	T
y	f	i	v	**E**	F	A	I	S
e	l	e	t	D	L	T	N	G
t	e	r	s	C	E	E	U	V
l	o	n	g	B	O	W	U	L

CHECKERBOARD (60-90 pairs)

A 5x5 Polybius square is used. In the simpler case one 5-letter keyword is to the left of the square and one above it (a). In the complex case, two 5-letter keywords are above and to the left. A plaintext letter is represented by two letters: its coordinates, in row/column order, from outside the square.

(a)

	W	H	I	T	E
B	K	N	I	G	H
L	P	Q	R	S	T
A	O	Y	Z	U	A
C	M	X	W	V	B
K	L	F	E	D	C

(b)

		G	R	A	Y	S
		W	H	I	T	E
H	B	K	N	I	G	H
O	L	P	Q	R	S	T
R	A	O	Y	Z	U	A
S	C	M	X	W	V	B
E	K	L	F	E	D	C

Example using square (a).

pt: n u m b e r s c a n a l s o b e u
CT(a): BH AT CW CE KI LI LT KE AE BH AE KW LT AW CE KI AT

pt: s e d a s c o o r d i n a t e s
CT(a): LT KI KT AE LT KE AW AW LI KT BI BH AE LE KI LT

CT(a):
BH AT CW CE KI LI LT KE AE BH AE KW LT AW CE KI AT LT KI KT AE LT KE AW AW LI KT BI BH AE LE KI LT.
or
BHATC WCEKI LILTK EAEBH AEKWL TAWCE KIATL TKIKT AELTK EAWAW LIKTB IBHAE LEKIL T.

Example using square (b).

pt: n u m b e r s c a n a l s o b e u
CT(b): HR RY CG SS EA LA OT KS RS BR AS EG LY AG CS EI AT

pt: s e d a s c o o r d i n a t e s
CT(b): LT KA ET RE OY EE RG AG LA KY HI HH RS OS EI LY

CT(b):
HR RY CG SS EA LA OT KS RS BR AS EG LY AG CS EI AT LT KA ET RE OY EE RG AG LA KY HI HH RS OS EI LY.
or
HRRYC GSSEA LAOTK SRSBR ASEGL YAGCS EIATL TKAET REOYE ERGAG LAKYH IHHRS OSEIL Y.

COMPLETE COLUMNAR TRANSPOSITION (period times 8-15 lines deep)
Written into a rectangular block by filling each row..

Taken out by columns in order of the key.

pt: filled block
Key: 312

3	1	2
f	i	l
l	e	d
b	l	o
c	k	x

CT: IELKL DOXFL BC.

CONDI (100 – 200 letters)

The Condi uses a simple keyed alphabet and keeps the word divisions. The encipherment process uses the position of the preceding plaintext letter in the keyed alphabet as the step distance along the alphabet to that plaintext letter's substitute.

With a starter value or off-set of #, substitute the first plaintext letter by the letter found # places further along the alphabet. Then the position of that first plaintext letter is the new value for #, the off-set for the next plaintext letter.

And so on.

Example: plaintext
pt: Ours is a very green pastime the wide variety of ciphers we use can all be solved with pencil and paper.

Keyword "STRANGE". The initial offset, #, is 25.

```
.........11111111112222222
12345678901234567890123456
STRANGEBCDFHIJKLMOPQUVWXYZ
```

CT: MIXA JJ N ZRDT NCDJH XWNRKAX CJP ADWM RZELQPS MR QVGSPDA XA TVB LIC GMG XK BPBHRM EDKJ NZHJVR QCK RWWZD."

CM BIFID (Conjugated Matrix Bifid) (150-200 letters) See: **BIFID**

	1	2	3	4	5
1	E	X	T	R	A
2	K	L	M	P	O
3	H	W	Z	Q	D
4	G	V	U	S	I
5	F	C	B	Y	N

pt

	1	2	3	4	5
1	N	C	D	R	S
2	O	B	F	Q	U
3	V	A	G	P	W
4	E	Y	H	M	X
5	L	T	I	K	Z

C T

pt: Odd periods are popular.

Proceed as for Bifid, but after reading out the numbers horizontally, substitute them with the letter found in the second 5x5 Polybius square. The keyword for the latter is NOVELTY, written in alternating verticals.

```
pt:     o d d p e r i   o d s a r e p   o p u l a r
row#:   2 3 3 2 1 1 4   2 3 4 1 1 1 2   2 2 4 2 1 1
col#:   5 5 5 4 1 4 5   5 5 4 5 4 1 4   5 4 3 2 5 4

CT: 23 32 11 45 55 41 45 23 41 11 25 54 54 14 22 42 11 54 32 54
CT: F  A  N  X  Z  E  X  F  E  N  U  K  K  R  B  Y  N  K  A  K
```

Ciphertext is usually written in period-length groups.

CT: FANXZEX FENUKKR BYNKAK.

DIGRAFID (120-220 letters)

A fractionated cipher using a tableau in which both alphabets are mixed. The plaintext is divided into digraphs, and the digraphs are written in groups, the number of digraphs in each group being the period of the cipher. Each digraph has a unique 3-digit number from the tableau and these are written vertically under the corresponding digraph. The 3-digit numbers are fractionated (as in a Trifid) and the new 3-digit numbers are put through the tableau to get the ciphertext digraphs. The first letter of the digraph is found in the horizontal alphabet, the second in the vertical, and the intersection number is placed between them.

1	2	3	4	5	6	7	8	9				
K	E	Y	W	O	R	D	A	B	1	2	3	
C	F	G	H	I	J	L	M	N	4	5	6	
P	Q	S	T	U	V	X	Z	#	7	8	9	
									v	d	p	1
									e	f	q	2
									r	g	s	3
									t	h	u	4
									i	j	w	5
									c	k	x	6
									a	m	y	7
									l	n	z	8
									b	o	#	9

pt: This is the forest pri

```
pt  (with fractionation 3*):
    Th Is Is   Th Ef Or   Es Tp Ri
     4  5  5    4  2  5    2  4  6
     8  6  6    8  2  1    3  9  1
     4  3  3    4  2  3    3  1  5
CT: Hj Mx Ws   Wj Ad Wg   Fc Sp Yi       CT: HJMXWS WJADWG FCSPYI.
```

```
pt (with fractionation 4**):
     Th Is Is Th   Ef Or Es Tp   Ri
      4  5  5  4    2  5  2  4    6
      8  6  6  8    2  1  3  9    1
      4  3  3  4    2  3  3  1    5
CT:  Hj Tk Vh Yu   Ff Wd Sq Yp   Ri      CT: HJTKVHYU FFWDSQYP RI.
```

*Fractionation 3 means 3 pairs of letters/6 letters.
** Fractionation 4 means 4 pairs of letters/8 letters.

FOURSQUARE (50-70 pairs)

Four 5x5 Polybius squares are set up. Squares 1 and 3 are plain unkeyed (I/J in same cell); squares 2 and 4 are keyed. In this example, squares 2 and 4 have a vertical route.

The first letter of each plaintext pair is found in square 1 and the second in square 3. The two cells are considered opposite corners of a rectangle. Cipher substitutes are found at the other corners of that rectangle, first in square 2 and the second in square 4.

		1					2		
A	B	C	D	E	G	R	D	L	U
F	G	H	I	K	E	Y	F	N	V
L	M	N	O	P	O	A	H	P	W
Q	R	S	T	U	M	B	I	Q	X
V	W	X	Y	Z	T	C	K	S	Z
L	I	C	N	V	A	B	C	D	E
O	T	D	P	W	F	G	H	I	K
G	H	E	Q	X	L	M	N	O	P
A	M	F	S	Y	Q	R	S	T	U
R	B	K	U	Z	V	W	X	Y	Z
		4					3		

pt: co me qu ic kl yw en ee dh el px
CT: LE WI XA FN EX CU DX UV DP GX HZ

CT: LE WI XA FN EX CU DX UV DP GX HZ.
or **LEWIX AFNEX CUDXU VDPGX HZ.**

FRACTIONATED MORSE (110-150 plaintext letters)

Each letter of the plaintext is first enciphered using Morse code with "x" between letters and "xx" between words. (xxx does not exist.) Normally punctuation is not enciphered, but for clarity or variation it may be added at the constructor's discretion. Morse code letters, numbers, and punctuation can be found in Appendix 1.

pt: c o m e a t o n c e.
MC:
– · – · x – – – x – – x · x x · – x – x x – – – x – · x – · – · x
· x x

This series of dots, dashes, x's is taken off in units of three, each trigraph set vertically and cipher letters assigned to each group using a keyword alphabet:

R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X	Y	Z
·	·	·	·	·	·	·	·	·	–	–	–	–	–	–	–	–	–	x	x	x	x	x	x	x	x
·	·	·	–	–	–	x	x	x	·	·	·	–	–	–	x	x	x	·	·	·	–	–	–	x	x
·	–	x	·	–	x	·	–	x	·	–	x	·	–	x	·	–	x	·	–	x	·	–	x	·	–

```
    – · – – · · – – x x – ·
    · x – – x – x – – – · x
    – – x x x x x – · · x x
CT: C B I I L T M H V V F L.
```

CT: CBIIL TMHVV FL.

GRANDPRÉ (150-200 plaintext letters)

An 8x8 square is filled with 8-letter words horizontally. The first letter of each word when reading vertically must form a ninth word. Each plaintext letter is represented by a 2-digit number; the coordinates are taken from the square. A letter appearing more than once in the square may be represented by more than one digit-pair. Unless otherwise specified, ALL 26 letters appear in the square.

While an 8x8 square is traditional and preferred, it is not required. The square can be no smaller than 6x6 and no bigger than 10x10. In the case of the 10x10, words are numbered 0-9.

	1	2	3	4	5	6	7	8
1	L	A	D	Y	B	U	G	S
2	A	Z	I	M	U	T	H	S
3	C	A	L	F	S	K	I	N
4	Q	U	A	C	K	I	S	H
5	U	N	J	O	V	I	A	L
6	E	V	U	L	S	I	O	N
7	R	O	W	D	Y	I	S	M
8	S	E	X	T	U	P	L	Y

pt: The first column is the keyword.

pt:	t	h	e	f	i	r	s	t	c	o	l	u	m
CT:	**84**	**27**	**82**	**34**	**56**	**71**	**77**	**26**	**44**	**54**	**64**	**63**	**78**

pt:	n	i	s	t	h	e	k	e	y	w	o	r	d
CT:	**52**	**66**	**65**	**84**	**27**	**82**	**36**	**61**	**88**	**73**	**54**	**71**	**13.**

GRILLE (12x12 square maximum)

Position 1: Perforations are shown. First quarter of the message is written in across.
Position 2: Turn the grille 90 degrees clockwise. Second quarter of the message is written in.
Position 3: Grille is turned 180 degrees clockwise from its original position. Third quarter of the message is written in.
Position 4: Grille is turned 270 degrees clockwise from its original position. Final quarter of the message is written in.

pt: the turning grille

```
X · · ·       t · · ·        · · · u       · · · ·       · i l ·
· · · X       · · · h        · r · ·       n · g ·       · · · ·
· X · X       · e · t        · · · ·       g · · ·       · · l ·
· · · ·       · · · ·        · n i ·       · · · r      e · · ·
Grille     Position 1     Position 2    Position 3    Position 4
```

```
CT:  T I L U
     N R G H
     G E L T
     E N I R
```

CT: TILUN RGHGE LTENI R.

This grille would be reported in the sols as "1 8 10 12".

GROMARK (100-150 letters) (**GRO**nsfeld with **M**ixed **A**lphabet and **R**unning **K**ey)

Set up as a K2M with columns taken off the transposition block in alphabetical order (See Keywords in Chapter 8). A 5-digit primer is chosen and a running numerical key is formed by adding successive pairs of digits (dropping 10's). The 1st plus 2nd give the 6th, 2nd plus 3rd give 7th, etc. Applying the key to the plaintext, the digit determines how far to the right to count before finding the substitute in the cipher alphabet. Then the ciphertext is written in 5-letter groups with the primer before the first group and the last digit after the last letter as a check.

Key: ENIGMA (264351)

Primer: 23452

Transposition block

2	6	4	3	5	1
E	N	I	G	M	A
B	C	D	F	H	J
K	L	O	P	Q	R
S	T	U	V	W	X
Y	Z				

alphabets:

pt: a b c d e f g h i j k l m n o p q r s t u v w x y z

CT: A J R X E B K S Y G F P V I D O U M H Q W N C L T Z

encipherment: **K:** 23452579772664982037023072537978066

pt: thereareuptotensubstitutesperletter

CT: NFYCKBTIJCNWZYCACJNAYNLQPWWSTWPJQFL

CT: 23452 NFYCK BTIJC NWZYC ACJNA YNLQP WWSTW PJQFL 6.

GRONSFELD (period times 12-15 lines deep)

This one is enciphered just like the Vigenère. The key is limited.
CT = K+pt. [Cipher = Key + Plaintext]

pt: This one uses ten of the twenty-six Vigenère alphabets.
Key: 9321492, period 7

key	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

```
Key:   9 3 2 1 4 9 2
       t h i s o n e        C K K T S W G
       u s e s t e n        D V G T X N P
       o f t h e t w        X I V I I C Y
pt:    e n t y s i x   CT:  N Q V Z W R Z
       v i g e n e r        E L I F R N T
       e a l p h a b        N D N Q L J D
       e t s                N W U
```

CT: CKKTS WGDVG TXNPX IVIIC YNQVZ WRZEL IFRNT NDNQL JDNWU.

HEADLINES (Five headlines from recent news)

The five headlines are encrypted using simple substitution with the same mixed alphabet at different settings against itself, as with a K3 key.

The mixed alphabet derives from a keyword alphabet, mixed by taking columns from a transposition block in a sequence determined by a second keyword. Cipher settings are determined by a third keyword.

Key Block:

```
A P O T H E C A R Y   Hat = APOTHECARY
1 7 6 9 5 4 3 2 8 10
C H E M I S T A B D   Key = CHEMIST
F G J K L N O P Q R
U V W X Y Z
```

Substitution Block:

```
   1     2   3   4     5     6     7     8   9     10
   C F U A P T O S N Z I L Y E J W H G V B Q M K X D R  pt

1  D R C F U A P T O S N Z I L Y E J W H G V B Q M K X  CT
2  R C F U A P T O S N Z I L Y E J W H G V B Q M K X D
3  U A P T O S N Z I L Y E J W H G V B Q M K X D R C F
4  G V B Q M K X D R C F U A P T O S N Z I L Y E J W H
5  S N Z I L Y E J W H G V B Q M K X D R C F U A P T O
   ^ Setting = DRUGS
```

The three keywords (HAT, KEY and SETTING) are related by context to aid in analysis when solving. At least two of the three keywords are required for SOL credit.

Hat: APOTHECARY **Key**: CHEMIST **Setting**: DRUGS

pt:

```
1. Bush Signs Intelligence Overhaul Legislation
2. Bin Laden Urges Fighters to Strike Oil Facilities
3. Pfizer: Painkiller may pose increased cardiovascular risk
4. Carrey masters disguises in 'Lemony Snicket'
5. Martinez blasts ex-teammate Schilling
```

CT:

```
1. *GCTJ TNWOT NOALZZNWLODL PHLXJFCZ ZLWNTZFANPO
2. *VZS *IUXYS FDHYO CZHWPYDO PT OPDZMY TZI CURZIZPZYO
3. *OAYLWF: OTYIDYEEWF XTJ ONZW YIUFWTZWC UTFCYNQTZUPETF FYZD
4. *GQHHPA YQDKPHD WFDNBFDPD FR '*UPYXRA *DRFGEPK'
5. *UIOYGWQH CVIJYJ QP-YQIUUIYQ *JSXGVVGWD
```

Variations of keying method include taking columns UP the transposition block, substituting with a plaintext block, and reading the setting UP the substitution block.

In case of identity encipherment, three reversals are made: columns are taken UP the transposition block, the setting reads UP the substitution block, and substitution is with a plaintext block (cipher alphabet on top of five plain alphabets).

HOMOPHONIC (50-75 pairs)

The plaintext alphabet is straight with I/J in the same cell. A plaintext or key letter J is replaced with I before encrypting. A 4-letter keyword determines where each of the number sequences will start in each row. 01-25 are in sequence in row 1, 26-50 in row 2, 51-75 in row 3, 76-00 in row 4. The keyword is given by 01, 26, 51, 76 (here GOLF). Each plaintext letter is enciphered by any of the 4 numbers below it.

A	B	C	D	E	F	G	H	I/J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	21	22	23	24	25	**01**	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19
38	39	40	41	42	43	44	45	46	47	48	49	50	**26**	27	28	29	30	31	32	33	34	35	36	37
66	67	68	69	70	71	72	73	74	75	**51**	52	53	54	55	56	57	58	59	60	61	62	63	64	65
96	97	98	99	00	**76**	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95

pt:	w o r d	d i v i s i o n s	m a y	b e	k e p t
CT:	16 26 11 99	69 46 33 03 88 79 54 83 12	06 38 94	67 24	04 00 27 89

CT:
16 26 11 99 69 46 33 03 88 79 54 83 12 06 38 94 67 24 04 00 27 89.

INCOMPLETE COLUMNAR TRANSPOSITION (period times 15-18 lines deep)

Written into block horizontally. Taken out by columns in order of key.

pt: Unfilled block
Key: 312

```
3 1 2
-----
u n f
i l l
e d b
l o c
k
```

CT: NLDOF LBCUI ELK.

INTERRUPTED KEY (40-60 letters)

The plaintext is enciphered with 1, 2, 3 or more letters of the keyword which is interrupted at random, by plaintext word division, or according to some other scheme. Return to the first key letter each time the keyword is interrupted. The entire keyword must be used at least once.

(Vigenère used in this example.)

pt: This cipher can be used with any of the periodics.
K: ORANGE

```
K:  O R A N  O R A N G E  O R  O R A  O R A N  O R A  O  O
pt: t h i s  c i p h e r  c a  n b e  u s e d  w i t  h  a
CT: H Y I F  Q Z P U K V  Q R  B S E  I J E Q  K Z T  V  O

K:  O R A N G  O  O R  O R A  O R A N G
pt: n y o f t  h  e p  e r i  o d i c s
CT: B P O S Z  V  S G  S I I  C U I P Y
```

CT: HYIFQ ZPUKV QRBSE IJEQK ZTVOB POSZ VSGSI ICUIP Y.

KEY PHRASE (75-100 letters)

The cipher alphabet is a 26-letter phrase which must be complete (not: TOBEORNOTOTBETHATISTHEQUES(tion)) and matched to a straight plaintext alphabet.

Word divisions are retained, and proper nouns and indicated by *.

Alphabets
pt: a b c d e f g h i j k l m n o p q r s t u v w x y z
CT: G I V E M E L I B E R T Y O R G I V E M E D E A T H

pt: a   c i p h e r t e x t   l e t t e r   m a y   s t a n d   f o r
CT: G   V B G I M V M M A M   T M M M M V   Y G T   E M G O E   E R V

pt: m o r e   t h a n   o n e   p l a i n t e x t   l e t t e r.
CT: Y R V M   M I G O   R O M   G T G B O M M A M   T M M M M V.

CT:
G   V B G I M V M M A M   T M M M M V   Y G T   E M G O E   E R V
Y R V M   M I G O   R O M   G T G B O M M A M   T M M M M V.

MONOME-DINOME (60-120 plaintext letters)

Choose a keyword for a 3x8 box, with I/J and two other letters (e.g. Y/Z) sharing entries. Place eight digits above the columns and the remaining two on the second and third rows of the box. The order of the digits may be selected with the box keyword or in any other way (for example, RMASTERTON
6318927054
Using the first two numbers as rows and the rest as column numbers).

	1	8	9	2	7	0	5	4
	N	O	T	A	R	I	E	S
6	B	C	D	F	G	H	K	L
3	M	P	Q	U	V	W	X	Y

Letters in the top row are encrypted with a single digit, the column digit, and letters in the second and third rows with the row digit followed by the column digit.

pt:	h	i	g	h	f	r	e	q	u	e	n	c	y	k	e	y	s	s	h	o	r
CT:	60	0	67	60	62	7	5	39	32	5	1	68	34	65	5	34	4	4	60	8	7

t	e	n	c	i	p	h	e	r	t	e	x	t
9	5	1	68	0	38	60	5	7	9	5	35	9

CT: 60067 60627 53932 51683 46553 44460 87951 68038 60579 5359.

MORBIT (50-75 plaintext letters)

Choose a 9-letter keyword to set up an array as shown. Plaintext is enciphered exactly as in the Fractionated Morse, x between letters, xx between words. The result is then taken off in units of 2, placed vertically, and numbers are taken from the array to form the ciphertext. Numbers represent alphabetical order of the key. (It is often as easy to read pairs horizontally as to rearrange them vertically.)

Key:

```
W I S E C R A C K
9 5 8 4 2 7 1 3 6
-----------------
· · · – – – x x x
· – x · – x · – x
```

pt: Once upon a time.

```
pt:   o      n       c     e   /    u        p       o       n
MC: – – – x – · x – · – · x · x x · · – x · – – · x – – – x – ·
CT: 2   7   4   3   5   8   8   1   5   1   2   8   2   7   4

 /  a    /  t    i     m    e
x x · – x x – x · · x – – x · x
6   5   6   7   9   3   7   8
```

CT: 27435 88151 28274 65679 378.

MYSZKOWSKI (period times 12-15 lines deep)

Choose a keyword with repeated letters. Number the letters in alphabetical order with repeated letters taking the same number as their first appearance. The plaintext is written in horizontally. The ciphertext is taken off by columns in key order.

pt: Incomplete columnar with pattern word key and letters under same number taken off by row from top to bottom.

Key: BANANA

```
B A N A N A    A A A B N N
2 1 3 1 3 1    1 1 1 2 3 3
--------------------------
i n c o m p    N O P I C M
l e t e c o    E E O L T C
l u m n a r    U N R L M A
w i t h p a    I H A W T P
t t e r n w    T R W T E N
o r d k e y    R K Y O D E
a n d l e t    N L T A D E
t e r s u n    E S N T R U
d e r s a m    E S M D R A
e n u m b e    N M E E U B
r t a k e n    T K N R A E
o f f b y r    F B R O F Y
o w f r o m    W R M O F O
t o p t o b    O T B T P O
o t t o m      T O   O T M
```

CT:

NOPEE OUNRI HATRW RKYNL TESNE SMNME TKNFB RWRMO TBTOI LLWTO ATDER OOTOC MTCMA TPEND EDERU RAUBA EFYFO POTM.

NICODEMUS (period times 15-18 lines deep)

Three steps are used:

1. Column transposition.
2. Vigenère encipherment with the same key.
3. Take off 5 letters at a time from each column in order.

Since last block maybe less than 5 deep, all remaining letters from each column are taken off in column order.

pt: the early bird gets the worm
Key: CAT

```
C A T    A C T    A C T
2 1 3    1 2 3    1 2 3
t h e    h t e    H V X
e a r    a e r    A G K
l y b    y l b    Y N U
i r d    r i d    R K W
g e t    e g t    E I M
s t h    t s h    T U A
e w o    w e o    W G H
r m      m r      M T
```

CT: HAYRE VGNKI XKUWM TWMUG TAH.

NIHILIST SUBSTITUTION (period times 8-12 lines deep)

A 5x5 Polybius square is used with a second keyword which also sets the period length. Each plaintext letter is designated by a 2-digit number, its row and column in the square. The message is written in period. Each plaintext letter is then replaced by the sum of its value (the 2-digit number) and the value of the key letter above it (found from the same square). Numbers from 100 to 110 are written 00 to 10.

	1	2	3	4	5
1	S	I	M	P	L
2	E	A	B	C	D
3	F	G	H	K	N
4	O	Q	R	T	U
5	V	W	X	Y	Z

pt: The early bird

Key: E A S Y
21 22 11 54
T H E E
44 33 21 21
65 55 32 75

A R L Y
22 43 15 54
43 65 26 08

B I R D
23 12 43 25
44 34 54 79

pt: t h e e a r l y b i r d
CT: 65 55 32 75 43 65 26 08 44 34 54 79.

NIHILIST TRANSPOSITION (10x10 maximum)

The same key is applied to rows and columns.

Enter the plaintext in square 1 by rows as shown. Transpose columns by key order into square 2. Transpose rows of square 2 by key order into square 3. The ciphertext is taken off by columns or rows from square 3.

pt: square needed here
Key: 2134

	1	2	3	4
1	S	Q	U	A
2	R	E	N	E
3	E	D	E	D
4	H	E	R	E

1

2	1	3	4
Q	S	U	A
E	R	N	E
D	E	E	D
E	H	R	E

2

	2	1	3	4
2	E	R	N	E
1	Q	S	U	A
3	D	E	E	D
4	E	H	R	E

3

Another option for encipherment follows. This method is described by **LEDGE** in *Novice Notes*. The results are the same for the ciphertext.

Enter the plaintext in square 1 by rows as shown. Transpose columns to numerical order in square 2. Transpose rows of square 2 to numberical key order into square 3. The ciphertext is taken off by columns or rows from square 3.

pt: square needed here
Key: 2134

	2	1	3	4
2	S	Q	U	A
1	R	E	N	E
3	E	D	E	D
4	H	E	R	E

1

1	2	3	4
Q	S	U	A
E	R	N	E
D	E	E	D
E	H	R	E

2

	1	2	3	4
1	E	R	N	E
2	Q	S	U	A
3	D	E	E	D
4	E	H	R	E

3

C1: EQDER SEHNU EREAD E. (taken off by columns)

or

C2: ERNEQ SUADE EDEHR E. (taken off by rows)

NULL (25-letter plaintext maximum)

This is a concealment cipher (a form of Steganography).

First letters, last letters, taken in order or reverse order, letters following each vowel, second letters in every other word, taking letters out of each word in a key order, e.g. 21534, etc. are some of the other ways a null may be constructed. In the following example, the middle letter of each word reveals the message.

pt: help

CT: THE GREAT OLD PUMPERS.

NUMBERED KEY (2.5 - 3 times the length of the extended key)

This is a substitution cipher.

To construct a numbered key cipher start with a key word, phrase, sentence, or paragraph, extend it by appending any missing letters in alphabetical order, then number the resulting extended key, perhaps starting in the middle of the key and wrapping around to the beginning. Each plaintext letter is then encrypted by one of the numbers in the key.

Key: "I like ciphers."

Extended key: i l i k e c i p h e r s a b d f g j m n o q t u v w x y z

Shifted extended key: m n o q t u v w x y z i l i k e c i p h e r s a b d f g j

Numbered key:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
m	n	o	q	t	u	v	w	x	y	z	i	l	i	k	e	c	i	p	h	e	r	s	a	b	d	f	g	j

Encryption table:

a 23	e 15, 20	i 11, 13, 17	m 0	q 3	u 5	y 9
b 24	f 26	j 28	n 1	r 21	v 6	z 10
c 16	g 27	k 14	o 2	s 22	w 7	
d 25	h 19	l 12	p 18	t 4	x 8	

Pt: The road to success is always under construction.

Worksheet:

04	19	20	21	02	23	25	04	02	22	05	16	16	15	22	22	11	22	23	12	07	23
t	h	e	r	o	a	d	t	o	s	u	c	c	e	s	s	i	s	a	l	w	a

09	22	05	01	25	20	21	16	02	01	22	04	21	05	16	04	17	02	01
y	s	u	n	d	e	r	c	o	n	s	t	r	u	c	t	i	o	n

CT:
**04 19 20 21 02 23 25 04 02 22 05 16 16 15 22 22 11 22 23 12 07 23
09 22 05 01 25 20 21 16 02 01 22 04 21 05 16 04 17 02 01.**

PERIODIC GROMARK (75-125 letters) See: **GROMARK**

The plaintext is written out in period determined by the key length (6 here). The numerical key from the transposition block (264351 here) is also used as the "chain-added" key. Keyword letters are written in order above each period group as shown below, repeating as needed. These key letters determine the starting position of the cipher alphabet for that particular group with each letter in the group shifting according to the chain-added key.

Key: ENIGMA (264351)

Transposition block

2	6	4	3	5	1
E	N	I	G	M	A
B	C	D	F	H	J
K	L	O	P	Q	R
S	T	U	V	W	X
Y	Z				

```
alphabets:
pt:  a b c d  e f g h i  j k l m  n o p q  r s t u  v w x y z
CT: (A J R X)(E B K S Y)(G F P V)(I D O U)(M H Q W)(N C L T Z)
     0        4          9        13       17       21
encipherment:

K:   E +4   N +21  I +13  G +9   M +17  A +0   E +4   N +21  I +13
pt: Wintry shower swillc ontinu eforth enextf ewdays accord ingtot
#:  264351 807869 875457 529922 718149 899537 784804 522849 740236
CT: RHNAAX NRUZBN IUARXC RTPATB RLIGDS VCIRCV OYPVRA AZZMUS REQYEV

K:   G +9   M +17
pt: hefore cast
#:  142597 5674
CT: MMURGW TLUD
```

CT:

264351 RHNAAX NRUZBN IUARXC RTPATB RLIGDS VCIRCV OYPVRA AZZMUS REQYEV MMURGW TLUD 4.

PHILLIPS (125-160 letters)

Starting with a basic 5x5 Polybius square (#1 below), the first row is shifted down one row at a time form squares #2, 3, 4 and 5. Row two is then shifted down a row at a time to form squares #6, 7 and 8. Each square is used in turn to encipher 5 plaintext letters. Each plaintext letter is enciphered by taking as substitute the letter diagonally down to the right using the proper square. A plaintext letter in the fifth column is replaced by the letter from the first column and the row below it; a plaintext letter in the fifth row is replaced by the letter in the first row and to its right.

pt: Squares one and five are actually the same as are squares two and eight. The overall period is forty.

Key: DIAGONALS

```
1  D I A G O      2  C B S L N      2  C B S L N      2  C B S L N
2  C B S L N      1  D I A G O      3  E F H K M      3  E F H K M
3  E F H K M      3  E F H K M      1  D I A G O      4  U T R Q P
4  U T R Q P      4  U T R Q P      4  U T R Q P      1  D I A G O
5  V W X Y Z      5  V W X Y Z      5  V W X Y Z      5  V W X Y Z
      #1                #2                #3                #4


2  C B S L N      3  E F H K M      3  E F H K M      3  E F H K M
3  E F H K M      2  C B S L N      4  U T R Q P      4  U T R Q P
4  U T R Q P      4  U T R Q P      2  C B S L N      5  V W X Y Z
5  V W X Y Z      5  V W X Y Z      5  V W X Y Z      2  C B S L N
1  D I A G O      1  D I A G O      1  D I A G O      1  D I A G O
      #5                #6                #7                #8
```

```
SQ     #1          #2          #3          #4          #5          #6
pt s q u a r   e s o n e   a n d f i   v e a r e   a c t u a   l l y t h
CT K Z W L Y   T G E D T   Q E T A R   B T Y G T   L F X W L   P P O X L

SQ     #7          #8          #1          #2          #3          #4
pt e s a m e   a s a r e   s q u a r   e s t w o   a n d e i   g h t t h
CT T Y K U T   K G K Y T   K Z W L Y   T G X S E   Q E T I R   Z Q A A Q

SQ     #5          #6          #7          #8        #1
pt e o v e r   a l l p e   r i o d i   s f o r t    y
CT T C I T Y   K P P V B   L H E F H   G R E Y X    O
```

CT:
KZWLY TGEDT QETAR BTYGT LFXWL PPOXL TYKUT KGKYT KZWLY TGXSE QETIR ZQAAQ TCITY KPPVB LHEFH GREYX O.

PHILLIPS-RC (150-180 letters) See: **PHILLIPS**

Encrypted like Phillips, but with both columns and rows shifted for each new key block.

pt: Squares one and five are actually the same as are squares two and eight. The overall period is forty.

Key: DIAGONALS

	1	2	3	4	5
1	D	I	A	G	O
2	C	B	S	L	N
3	E	F	H	K	M
4	U	T	R	Q	P
5	V	W	X	Y	Z

#1

	2	1	3	4	5
2	B	C	S	L	N
1	I	D	A	G	O
3	F	E	H	K	M
4	T	U	R	Q	P
5	W	V	X	Y	Z

#2

	2	3	1	4	5
2	B	S	C	L	N
3	F	H	E	K	M
1	I	A	D	G	O
4	T	R	U	Q	P
5	W	X	V	Y	Z

#3

	2	3	4	1	5
2	B	S	L	C	N
3	F	H	K	E	M
4	T	R	Q	U	P
1	I	A	G	D	O
5	W	X	Y	V	Z

#4

	2	3	4	5	1
2	B	S	L	N	C
3	F	H	K	M	E
4	T	R	Q	P	U
5	W	X	Y	Z	V
1	I	A	G	O	D

#5

	3	2	4	5	1
3	H	F	K	M	E
2	S	B	L	N	C
4	R	T	Q	P	U
5	X	W	Y	Z	V
1	A	I	G	O	D

#6

	3	4	2	5	1
3	H	K	F	M	E
4	R	Q	T	P	U
2	S	L	B	N	C
5	X	Y	W	Z	V
1	A	G	I	O	D

#7

	3	4	5	2	1
3	H	K	M	F	E
4	R	Q	P	T	U
5	X	Y	Z	W	V
2	S	L	N	B	C
1	A	G	O	I	D

#8

SQ	**#1**	**#2**	**#3**	**#4**	**#5**	**#6**
pt	s q u a r	e s o n e	a n d f i	v e a r e	a c t u a	l l y t h
CT	K Z W L Y	R G F I R	U F Q A R	N P Y G P	L F X W L	P P O Y B

SQ	**#7**	**#8**	**#1**	**#2**	**#3**	**#4**
pt	e s a m e	a s a r e	s q u a r	e s t w o	a n d e i	g h t t h
CT	R Y K U R	K G K Y R	K Z W L Y	R G V C F	U F Q G R	V Q A A Q

SQ	**#5**	**#6**	**#7**	**#8**	**#1**
pt	e o v e r	a l l p e	r i o d i	s f o r t	y
CT	T C I T Y	F P P V S	L M E H M	G U F Y V	O

CT:

KZWLY RGFIR UFQAR WPYGP LFXWL PPOYB RYKUR KGKYR KZWLY RGVCF UFQGR VQAAQ TCITO FPPVS LMEHM GUFYV O.

PLAYFAIR (40-50 pairs)

A 5x5 Polybius square is used. The plaintext is separated into pairs. Double letters in a pair require insertion of a null between them.

Encipher by pairs:

1. When the 2 letters are in the same column of the keysquare, each is enciphered by the letter directly below it. Bottom cycles to the top.

2. When the two plaintext letters are in the same row, each is enciphered by the letter directly to its right. The last letter on the right cycles to the first letter in the same row.

3. When 2 letters are in different rows and columns, they are enciphered by the 2 letters which form a rectangle with them, beginning with the letter in the same row as the first letter of the pair.

L	O	G	A	R
I	T	H	M	B
C	D	E	F	K
N	P	Q	S	U
V	W	X	Y	Z

pt: co me qu ic kl yw en ex ed he lp
CT: DL HF SN CN CR ZX CQ QG FE EQ ON.

POLLUX (80-100 plaintext letters)

Each digit from 0 to 9 represents a dot, dash, or a divider. Two dividers are used to separate words. We usually use 4 dots and 3 of the other symbols in any order. Morse code alphabet is used.

The best solving procedure is to try to locate the x's, remembering that 3 x's in a row are impossible. Because of the length of Morse characters, either the second, third, fourth, or fifth number in the ciphertext must be a divider (unless special signs or numbers are used).

1	2	3	4	5	6	7	8	9	0
x	-	·	·	x	·	-	-	x	·

pt: Luck helps.

Morse code: ·-··x··-x-·-·x-·-xx····x·x·-··x·--·x···

CT: 08639 34257 02417 68596 30414 56234 90874 5360.

PORTA (period times 10-15 lines deep)

This periodic uses only 13 alphabets. The first half (A-M) is reciprocal with the second half. The position of the second half is determined by a key designation (A,B or C,D, etc.). The keys are used in the keyword which also determines the period. In the A,B alphabet, pt a = CT N, pt b = CT O, pt n = CT A, pt o = CT B, etc. In the C,D alphabet, pt a = CT O, pt o = CT A, etc.

Keys	A	B	C	D	E	F	G	H	I	J	K	L	M
A,B	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C,D	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
E,F	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
G,H	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
I,J	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
K,L	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
M,N	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
O,P	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
Q,R	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
S,T	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
U,V	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
W,X	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
Y,Z	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

pt: encipherment is reciprocal

Key: PORTA

K =	P	O	R	T	A						
pt=	e	n	c	i	p	**CT**=	Y	G	X	R	C
	h	e	r	m	e		O	Y	J	V	R
	n	t	i	s	r		G	M	Q	J	E
	e	c	i	p	r		Y	W	Q	G	E
	o	c	a	l			H	W	V	U	

CT: YGXRC OYJVR GMQJE YWQGE HWVU.

PORTAX (period times 16-24 lines deep, 8-12 lines paired)

A slide is made up of two alphabets which have been labeled A1 and A2 in the diagram below. The fixed part of the slide contains the first half of the alphabet (A-M). The bottom row of the slide consists of the second half of the alphabet (N-Z). The second alphabet is written below in columns of two characters. The sequence on the sliding part repeats to allow for the slide.

```
                    A B C D E F G H I J K L M        A1/1 (fixed)
N O P Q R S T U V W X Y Z N O P Q R S T U V W X Y Z  A1/2
                                                        (sliding)
A C E G I K M O Q S U W Y A C E G I K M O Q S U W Y  A2
B D F H J L N P R T V X Z B D F H J L N P R T V X Z
```

Enciphering is by pairs. The message is written horizontally into a block under a keyword. Vertical pairs are enciphered. The first letter of the pair (top) is found in the upper alphabet (A1/1 OR A1/2), the second is found in the lower one (A2). These are taken as diagonally opposite corners of a rectangle. The other corners are taken as the substitutes, the letter from the top being taken first. If the two letters are on the same vertical line, the other two letters on that line are the substitutes.

The slide shown is set for the key letters U or V (found below A of the upper part of the top alphabet). Using that key, "in" becomes JL, "no" becomes UA, and "na" becomes DB. The resulting cipher is taken off by horizontal rows.

pt: the early bird gets the worm

K: EASY

```
K =  E A S Y

pt = t h e e    CT = N I J A
     a r l y         M P B G
     b i r d         Q C W K
     g e t s         H Q J E
     t h e w         U I K Y
     o r m x         M P A T
```

CT: NIJAM PBGQC WKHQJ EUIKY MPAT.

PROGRESSIVE KEY (100-150 letters)

The plaintext is set up in period length groups. Ordinary periodic (here Vigenère) encipherment using the keyword yields a "primary" ciphertext as shown below just under the plaintext. Then a second encipherment of the same type using a progressing key letter (Kp) for each group gives the final ciphertext. For a progression index of 1, the derived progressive key for the second encipherment is A for the first group, B for the second group, etc. For a progression index of 2, the progressive key would be A, C, E, etc. for successive groups.

Key: GRAPEFRUIT, period 10

```
 K: G R A P E F R U I T  G R A P E F R U I T  G R A P E F R U I T
pt: t h i s c i p h e r  c a n b e u s e d w  i t h a n y o f t h
C1: Z Y I H G N G B M K  I R N Q I Z J Y L P  O K H P R D F Z B A
Kp:          A                    B                    C
C2: Z Y I H G N G B M K  J S O R J A K Z M Q  Q M J R T F H B D C
```

CT: ZYIHG NGBMK JSORJ AKZMQ QMJRT FHBDC NJHJP WXFNO.

QUAGMIRE I (period times 15-18 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus, a Quagmire 1 uses a K1 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: The Quag One is a periodic cipher with a keyed plain alphabet run against a straight cipher alphabet.

Key: SPRINGFEV(ER)
Indicator key under ***A*** is **FLOWER** (period 6).

Keyed	pt	**S**	**P**	**R**	**I**	**N**	**G**	**F**	**E**	**V**	***A***	B	C	D	H	J	K	L	M	O	Q	T	U	W	X	Y	Z
C	1	W	X	Y	Z	A	B	C	D	E	**F**	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
I	2	C	D	E	F	G	H	I	J	K	**L**	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
P	3	F	G	H	I	J	K	L	M	N	**O**	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
H	4	N	O	P	Q	R	S	T	U	V	**W**	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
E	5	V	W	X	Y	Z	A	B	C	D	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
R	6	I	J	K	L	M	N	O	P	Q	**R**	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H

```
       1 2 3 4 5 6
pt:    t h e q u a     CT:    Q P M G Q R
       g o n e i s            B U J U Y I
       a p e r i o            F D M P Y A
       d i c c i p            I F Q Y Y J
       h e r w i t            J J H J Y C
       h a k e y e            J L U U T P
       d p l a i n            I D V W Y M
       a l p h a b            F S G A E S
       e t r u n a            D W H I Z R
       g a i n s t            B L I R V C
       a s t r a i            F C Z P E L
       g h t c i p            B P Z Y Y J
       h e r a l p            J J H W L J
       h a b e t              J L P U P
```

CT:
QPMGQ RBUJU YIFDM PYAIF QYYJJ JHJYC JLUUT PIDVW YMFSG AESDW HIZRB LIRVC FCZPE LBPZY YJJJH WLJJL PUP.

QUAGMIRE II (period times 15-18 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 2 uses a K2 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: In the Quag Two a straight plain alphabet is run against a keyed cipher alphabet.

Key: SPRINGFEV(ER)
Indicator key under plaintext alphabet ***A*** is **FLOWER** (period 6).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	**pt**
1	**F**	**E**	**V**	A	B	C	D	H	J	K	L	M	O	Q	T	U	W	X	Y	Z	**S**	**P**	**R**	**I**	**N**	**G**	
2	**L**	M	O	Q	T	U	W	X	Y	Z	**S**	**P**	**R**	**I**	**N**	**G**	**F**	**E**	**V**	A	B	C	D	H	J	K	
3	**O**	Q	T	U	W	X	Y	Z	**S**	**P**	**R**	**I**	**N**	**G**	**F**	**E**	**V**	A	B	C	D	H	J	K	L	M	**CT**
4	**W**	X	Y	Z	**S**	**P**	**R**	**I**	**N**	**G**	**F**	**E**	**V**	A	B	C	D	H	J	K	L	M	O	Q	T	U	
5	**E**	V	A	B	C	D	H	J	K	L	M	O	Q	T	U	W	X	Y	Z	**S**	**P**	**R**	**I**	**N**	**G**	**F**	
6	**R**	**I**	**N**	**G**	**F**	**E**	**V**	A	B	C	D	H	J	K	L	M	O	Q	T	U	W	X	Y	Z	**S**	**P**	

```
      1 2 3 4 5 6
pt:   i n t h e q     CT:   J I C I C O
      u a g t w o           S L Y K I L
      a s t r a i           F V C H E B
      g h t p l a           D X C C O R
      i n a l p h           J I O E W A
      a b e t i s           F M W K K T
      r u n a g a           X B G W H R
      i n s t a k           J I B K E D
      e y e d c i           B J W Z A B
      p h e r a l           U X W H E H
      p h a b e t           U X O X C U
```

CT:
JICIC OSLYK ILFVC HEBDX CCORJ IOEWA FMWKK TXBGW HRJIB KEDBJ WZABU XWHEH UXOXC U.

QUAGMIRE III (period times 20-25 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 3 uses a K3 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: The same keyed alphabet is used for plain and cipher alphabets.
Key: AUTOMOBILE
Indicator key shown here under plaintext ***A* is HIGHWAY** (period 7).

	A	**U**	**T**	**O**	**M**	**B**	**I**	**L**	**E**	C	D	F	G	H	J	K	N	P	Q	R	S	V	W	X	Y	Z	**pt**
1	**H**	J	K	N	P	Q	R	S	V	W	X	Y	Z	A	U	T	O	M	B	I	L	E	C	D	F	G	
2	**I**	L	E	C	D	F	G	H	J	K	N	P	Q	R	S	V	W	X	Y	Z	A	U	T	O	M	B	
3	**G**	H	J	K	N	P	Q	R	S	V	W	X	Y	Z	A	U	T	O	M	B	I	L	E	C	D	F	**CT**
4	**H**	J	K	N	P	Q	R	S	V	W	X	Y	Z	A	U	T	O	M	B	I	L	E	C	D	F	G	
5	**W**	X	Y	Z	A	U	T	O	M	B	I	L	E	C	D	F	G	H	J	K	N	P	Q	R	S	V	
6	**A**	U	T	O	M	B	I	L	E	C	D	F	G	H	J	K	N	P	Q	R	S	V	W	X	Y	Z	
7	**Y**	Z	A	U	T	O	M	B	I	L	E	C	D	F	G	H	J	K	N	P	Q	R	S	V	W	X	

	1	2	3	4	5	6	7								
pt:	t	h	e	s	a	m	e	**CT:**	K	R	S	L	W	M	I
	k	e	y	e	d	a	l		T	J	D	V	I	A	B
	p	h	a	b	e	t	i		M	R	G	Q	M	T	M
	s	u	s	e	d	f	o		L	L	I	V	I	F	U
	r	p	l	a	i	n	a		I	X	R	H	T	N	Y
	n	d	c	i	p	h	e		O	N	V	R	H	H	I
	r	a	l	p	h	a	b		I	I	R	M	C	A	O
	e	t	s						V	E	I				

CT: KRSLW MITJD VIABM RGQMT MLLIV IFUIX RHTNY ONVRH HIIIR MCAOV EI.

QUAGMIRE IV (period times 25-30 lines deep)

The Quagmires are numbered in the same way as keywords (See Chapter 8). Thus a Quagmire 4 uses a K4 keyword plan. An indicator keyword is also used to determine the period and the ciphertext alphabet settings. It may appear vertically under any letter of the plaintext alphabet. The encipherments follow each letter of the indicator key in turn.

pt: This one employs three keywords
Key: (pt): SENSORY, (CT): PERC(EP)TION
Indicator shown here under plaintext ***S*** is **EXTRA** (period 5).

	S	**E**	**N**	**O**	**R**	**Y**	A	B	C	D	F	G	H	I	J	K	L	M	P	Q	T	U	V	W	X	Z	**pt**
1	**E**	**R**	**C**	**T**	**I**	**O**	**N**	A	B	D	F	G	H	J	K	L	M	Q	S	U	V	W	X	Y	Z	**P**	
2	**X**	Y	Z	**P**	**E**	**R**	**C**	**T**	**I**	**O**	**N**	A	B	D	F	G	H	J	K	L	M	Q	S	U	V	W	
3	**T**	I	O	N	A	B	D	F	G	H	J	K	L	M	Q	S	U	V	W	X	Y	Z	**P**	**E**	**R**	**C**	**CT**
4	**R**	**C**	**T**	**I**	**O**	**N**	A	B	D	F	G	H	J	K	L	M	Q	S	U	V	W	X	Y	Z	P	E	
5	**A**	B	D	F	G	H	J	K	L	M	Q	S	U	V	W	X	Y	Z	**P**	**E**	**R**	**C**	**T**	**I**	**O**	**N**	

	1	2	3	4	5						
pt:	t	h	i	s	o	**CT:**	V	B	M	R	F
	n	e	e	m	p		C	Y	I	S	P
	l	o	y	s	t		M	P	B	R	R
	h	r	e	e	k		H	E	I	C	X
	e	y	w	o	r		R	R	E	I	G
	d	s					D	X			

CT: VBMRF CYISP MPBRR HEICX RREIG DX.

RAGBABY (80-150 letters)

Historically the Ragbaby has used a 24-letter keyed alphabet. A 26- or 36-letter keyed-alphabet could be used.

Construct a 24-letter keyed alphabet (KA) with I/J and W/X paired:
KA: G R O S B E A K C D F H I L M N P Q T U V W Y Z

If J or X appears in the keyword it may be replaced with I or W, respectively; however, it is preferable to choose a key that uses neither letter.

A hyphenated word is considered a single word, as is a word with an apostrophe.

Example 1:

```
pt: t w o - s q u a r e
 #: 2 3 4   5 6 7 8 9 10
```

Example 2:

pt: Word divisions are kept.

Number the letters of each plaintext word in sequence beginning with 1 for the first letter of the first word, 2 for the first letter of the second word, etc. The sequence goes to 24 and repeats (25=1). Each plaintext letter is enciphered by moving to the right the designated number of spaces, using the letter found there as its substitute.

```
pt: w o r d  d i v i s i o n s  a r e  k e p t
#:  1 2 3 4  2 3 4 5 6 7 8 9 10 3 4 5  4 5 6 7
CT: Y B B L  H N G Q D U F G L  D E F  H F Y R.
```

RAILFENCE (3-7 rows, 10-15 times number of rows)

The plaintext may start at any point on the cycle, is written in zig-zag, and is taken off by rows or vice versa.

Key types are indicated in the solutions.
For example: "4 0" indicates four rows and no offset. Offsets run from 0 to 2R-3, where R is the number of rows.

pt: Civil war field cipher.

```
c       l       f       d       h
  i   i   w   r   i   l   c   p   e
    v       a       e       i       r
```

CT: CLFDH IIWRI LCPEV AEIR.

REDEFENCE (3-7 rows, 10-15 times the number of rows)

The plaintext may start at any point in the cycle, is written in zig-zag, and is taken off by rows according to a key (here 213).

Key types are indicated in the solutions.
For example: "3 2" indicates three rows and an offset of 2.

pt: `Civil war field cipher.`

```
 2: c   l   f   d   h
 1:  i i w r i l c p e
 3:   v   a   e   i   r
```

CT: IIWRI LCPEC LFDHV AEIR.

ROUTE TRANSPOSITION (8x8 square maximum, 8x10 rectangle maximum)

There are many routes and combinations of routes from which to choose: horizontal, vertical, alternating horizontal, alternating vertical, diagonal, alternating diagonal, clockwise inward spiral, counterclockwise inward spiral, clockwise outward spiral, and counterclockwise outward spiral. Don’t forget about the various starting positions!

This example is written into the block by alternating diagonals and taken out by clockwise spiral. The block must be complete.

pt: there are many routes

```
t h a
e e r
r e y
m n r
a o e
u t s
```

CT: THARY RESTU AMREE ENO.

RUNNING KEY (40-50 letters)

The plaintext is divided in half and written in two rows, one under the other. The top half acts as the key, the bottom half acts as the plaintext and the encipherment is the cipher. (Vigenère is used with this example.)

pt: This cipher can be used with any of the periodics.

Key: T H I S C I P H E R C A N B E U S E D W
pt: i t h a n y o f t h e p e r i o d i c s
CT: B A P S P G D M X Y G P R S M I V M F O

CT: BAPSP GDMXY GPRSM IVMFO.

SERIATED PLAYFAIR (10-15 groups paired) See: **PLAYFAIR**

The plaintext is written horizontally in 2-line periodic groups. This is shown below in period 6.

```
pt: Come quickly we need help immediately. tom.
```

```
pt: comequ eneedh mediat
    icklyw xelpim elytom
```

Vertical pairs thus formed are enciphered by the Playfair rules (1-3). When a vertical pair would be a double letter a null is inserted. Using the 5x5 Polybius square

```
L O G A R
I T H M B
C D E F K
N P Q S U
V W X Y Z
```

```
pt:   comequ eneedh mediat
      icklyw xelpim elytom
```

gives

```
CT:   NLBCSP QQCDCM HCFTRH
      CDFGXZ GCGQTB FGWHGB.
```

The cipher is taken off horizontally in 5-letter groups.

```
CT:  NLBCS PCDFG XZQQC DCMGC GQTBH CFTRH FGWHG B.
```

SLIDEFAIR (key length times 10-18 lines deep)

Enciphering is done in pairs. A keyword is used to fix the period. **Period length is the length of the keyword.** The first plaintext letter is found in the top alphabet and the second in one of the lower alphabets, depending on which letter of the keyword is in use. The plaintext pair is thought of as forming diagonally opposite corners of a rectangle. The letters from the other corners are the substitutes, that from the top taken first. If the letters form a vertical pair in the alphabets, the cipher equivalent is the pair just to the right.

Abbreviated Vigenère Table:

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

Abbreviated Variant Table:

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Abbreviated Beaufort Table:

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C

For example: Using the abbreviated tables found above, if the **key letter is B**, then

		Vigenère CT	**Variant CT**	**Beaufort CT**
pt	ca becomes	**ZD**	**BB**	**BZ**
pt	de becomes	**EF**	**FC**	**XY**

The following example uses Vigenère encipherment.

Key: DIGRAPH

pt: The Slidefair can be used with Vigenère **,** Variant or Beaufort**.**

K:	**D**	**I**	**G**	**R**	**A**	**P**	**H**							
pt:	th	es	li	de	fa	ir	ca	**CT:**	EW	KM	CR	NU	AF	CX	TJ
	nb	eu	se	dw	it	hv	ig		YQ	MM	YY	FU	TI	GW	ZP
	en	er	ev	ar	ia	nt	or		KH	JM	PK	BS	AI	EC	KV
	be	au	fo	rt					CF	MI	IL	CI			

CT:
EW KM CR NU AF CX TJ YQ MM YY FU TI GW ZP KH JM PK BS AI EC KV CF MI IL CI.

SWAGMAN (3-6 times key square)

A transposition cipher. Pick a random numerical key of 4-8 digits. Make a key square using the same digits randomly with no row or column containing a repeated number. Plaintext is written horizontally to complete a rectangle, using nulls if necessary. Ciphertext is formed by placing plaintext letters into the cipher squares vertically in order of key numbers. The final cipher is taken off vertically.

pt: Don't be afraid to take a big leap if one is indicated. You cannot cross a river or a chasm in two small jumps.

Key: 32145

```
pt:  D O N T B   E A F R A   I D T O T   A K
     E A B I G   L E A P I   F O N E I   S I
     N D I C A   T E D Y O   U C A N N   O T
     C R O S S   A R I V E   R O R A C   H A
     S M I N T   W O S M A   L L J U M   P S


K:   3 2 1 4 5   3 2 1 4 5   3 2 1 4 5   3 2
     1 5 3 2 4   1 5 3 2 4   1 5 3 2 4   1 5
     2 4 5 3 1   2 4 5 3 1   2 4 5 3 1   2 4
     5 3 4 1 2   5 3 4 1 2   5 3 4 1 2   5 3
     4 1 2 5 3   4 1 2 5 3   4 1 2 5 3   4 1

CT:  E M N S A   L O F V O   F L T A N   S S
     N O I I S   T A S P E   U D J E C   O K
     D R B C T   E R A Y A   I O N N M   A A
     S D O T G   W E I R I   L C R O I   P T
     C A I N B   A E D M A   R O A U T   H I
```

CT:
ENDSC MORDA NIBOI SICTN ASTGB LTEWA OAREE FSAID VPYRM OEAIA FUILR LDOCO TJNRA AENOU NCMIT SOAPH SKATI.

SYLLABARY (110-154 ciphertext pairs)

As with the ACA's Checkerboard, the row/column coordinates (CT) may be scrambled, the keysquare (pt) may be scrambled (by keyword and/or fill pattern), or the coordinates and Plaintext alphabet may both be scrambled. These variants are identified as “Unknown Coordinates, Known Keysquare,” “Known Coordinates, Unknown Keysquare,” and “Unknown Coordinates, Unknown Keysquare,” respectively. “Known coordinates” should be entered using the sequence 0-9, left to right and top to bottom. A standard syllabary “alphabet” is shown in both mixed and unmixed forms in the appendices. Standard syllabaries for French and German ciphers can also be found in the appendices.

As when using 36-character alphabet in 6x6 Polybius Squares, digits must be placed immediately following their corresponding letters in the unmixed square. This convention applies to keyed alphabets as well, in which those elements of the “alphabet” not used in the keyword are placed into the square sequentially following the keyword elements.

An important feature of the syllabary cipher is the suppression of letter frequency and word patterns that are produced by many simple substitution ciphers. This is achieved by means of variant spellings (*isologs*) of the same plaintext. For example, using the keysquare below the plaintext element *ORDERS RECEIVED* could be encrypted in several ways:

	6	7	1	9	4	3	2	5	0	8
8	**C**	**3**	**H**	**8**	**AR**	**M**	**ING**	**P**	**RI**	**N**
5	**CE**	**A**	**1**	**AL**	**AN**	**AND**	**ARE**	**AS**	**AT**	**ATE**
0	**ATI**	**B**	**2**	**BE**	**CA**	**CO**	**COM**	**D**	**4**	**DA**
2	**DE**	**E**	**5**	**EA**	**ED**	**EN**	**ENT**	**ER**	**ERE**	**ERS**
3	**ES**	**EST**	**F**	**6**	**G**	**7**	**HAS**	**HE**	**I**	**9**
4	**IN**	**ION**	**IS**	**IT**	**IVE**	**J**	**Ø**	**K**	**L**	**LA**
1	**LE**	**ME**	**ND**	**NE**	**NT**	**O**	**OF**	**ON**	**OR**	**OU**
6	**Q**	**R**	**RA**	**RE**	**RED**	**RES**	**RO**	**S**	**SE**	**SH**
7	**ST**	**STO**	**T**	**TE**	**TED**	**TER**	**TH**	**THE**	**THI**	**THR**
9	**TI**	**TO**	**U**	**V**	**VE**	**W**	**WE**	**X**	**Y**	**Z**

Unknown coordinates, Unknown Keysquare

```
pt: o  r  d  e  r  s  r  e  c  e  i  v  e  d
CT: 13 67 05 27 67 65 67 27 86 27 30 99 27 05

pt: or de r  s  re ce ive d
CT: 10 26 67 65 69 56 44  05

pt: or d  er s  re ce i  ve d
CT: 10 05 25 65 69 56 30 94 05

pt: o  r  de r  s  r  e  c  e  i  v  ed
CT: 13 67 26 67 65 67 27 86 27 30 99 24
```

TRIDIGITAL (75-100 letters)

A 10-letter keyword is used to produce a numerical key which is placed above a block 10 columns wide. A keyword alphabet (26 letters) is written into the block leaving the last column blank. Each pt. letter is enciphered by the digit above it. The digit above the last column is used as a word separator.

```
N O V E L C R A F T
6 7 0 3 5 2 8 1 4 9
-------------------
D R A G O N F L Y -
B C E H I J K M P -
Q S T U V W X Z - -
```

```
pt: t h e   i d e s   o f   m a r c h
CT: 0 3 0 9 5 6 0 7 9 5 8 9 1 0 7 7 3.
```

CT: 03095 60795 89107 73.

TRIFID (120-150 letters) See: **TWIN TRIFID**

Start with a 27-letter alphabet (# as the 27th symbol). Select a period (5-15) and write plaintext in period length groups. Below each plaintext letter write its three coordinates vertically using the key array. Reading horizontally, replace each 3-digit number with the letter it represents from the keyword alphabet identified by its vertical coordinates in the array. Complete each period-length group before going on to the next, i.e., use second and third rows of numbers as shown by "/". The period of the example is 10.

```
1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 3 3 3 3 3 3 3 3 3
1 1 1 2 2 2 3 3 3 1 1 1 2 2 2 3 3 3 1 1 1 2 2 2 3 3 3
1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3
E X T R A O D I N Y B C F G H J K L M P Q S U V W Z #
```

```
pt: t r i f i d s a r e / f r a c t i o n a t / e d c i p h e r s
#:  1 1 1 2 1 1 3 1 1 1   2 1 1 2 1 1 1 1 1 1   1 1 2 1 3 2 1 1 3
 :  1 2 3 2 3 3 2 2 2 1   2 2 2 1 1 3 2 3 2 1   1 3 1 3 1 2 1 2 2
 :  3 1 2 1 2 1 1 2 1 1   1 1 2 3 3 2 3 3 2 3   1 1 3 2 2 3 1 1 1
CT: E Y M X V U C R Y Y / Y Y E A Y V Y O V V / X I T D P A T H E
```

Ciphertext is written in 5-letter groups or period length.

CT: EYMXV UCRYY YYEAY VYOVV XITDP ATHE.

TRI-SQUARE (100-125 groups)

Three 5x5 Polybius key squares are used. The plaintext is written in pairs. The first plaintext letter is found in square 1, the second in square 2. A ciphertext trigraph is formed for each plaintext digraph: Any letter in the same column with the first plaintext letter in square 1 may be used as the first cipher letter. The intersection in square 3 of the row containing the first plaintext letter in square 1 with the column containing the second plaintext letter in square 2 gives the second cipher letter. Any letter in the same row in square 2 as the second plaintext letter may be used as the third ciphertext letter.

								2		
						R	E	A	D	I
						N	G	B	C	F
						H	K	L	M	O
						P	Q	S	T	U
						V	W	X	Y	Z
	N	S	F	M	U	P	A	S	T	I
	O	A	G	P	W	N	O	Q	R	M
1	V	B	H	Q	X	L	Y	Z	U	E
	E	C	I	R	Y	K	X	W	V	B
	L	D	K	T	Z	H	G	F	D	C
								3		

pt: t h r e e k e y s q u a r e s u s e d x
CT: RHL QXR LXO EVZ BAT XSE RXD DIU AAA BFZ.

TWIN BIFID (100-150 letters each, 18 letter minimum repeat) See: **BIFID**

Two bifid messages using the same Polybius key square but with different periods, have a phrase of the plaintext in common. For use in the Cipher Exchange, it is recommended that one period be odd and one even.

TWIN TRIFID (100-150 letters each, 16 letter minimum repeat) See: **TRIFID**

Two trifid messages using the same key but with different periods, have a phrase of the plaintext in common. For use in the Cipher Exchange, it is recommended that one period be odd and one even.

TWO-SQUARE (45-65 pairs)

Two 5x5 Polybius squares are set up up. The message is divided into pairs. The first letter of each pair is found in square 1, the second in square 2. The cipher equivalents are those letters forming the opposite corners of a rectangle determined by the pt pair. If the plaintext letters are in the same row the cipher equivalents are the same letters reversed.

1

D	I	A	L	O
G	U	E	B	C
F	H	K	M	N
P	Q	R	S	T
V	W	X	Y	Z

2

B	I	O	G	R
A	P	H	Y	C
D	E	F	K	L
M	N	Q	S	T
U	V	W	X	Z

pt: an ot he rd ig ra ph ic se tu px
CT: IR RT EH MK GI ME QG RU NM MZ SV.

VARIANT (period times 10-15 lines deep)

The plaintext is written into a block under a key word. All letters in the first column are enciphered using the first key letter; the second column uses the second key letter, etc.

To encipher the example below: Find the first letter of the plaintext, c, look down the K (key) column of the tableau (See Appendix 3) for A and across the top (A, Plaintext) row for I. Where A's row meets c's column find the ciphertext, C.

pt: C equals P minus K.
Key: APPLE

```
 K:   A P P L E
      ---------
pt:   c e q u a     CT:   C P B J W
      l s p m i           L D A B E
      n u s k             N F D Z
```

CT: CPBJW LDABE NFDZ.

VIGENÈRE (period times 10-15 lines deep)

The plaintext is written into a block under the key.

For this example, the block is 14 across. All letters in the first column are enciphered using P as key, in the second using O, etc. Thus to encipher the first letter of the plaintext, **i**, look down the K (key) column of the tableau (See Appendix 2) for **P** and across the top (pt) row for **i**. Where **P**'s row meets **i**'s column find ciphertext **X**.

pt: In the Vigenère, C equals K plus P where A is zero, B is one, etc.

```
Key:    P O L Y A L P H A B E T I C
        i n t h e v i g e n e r e c
pt:     e q u a l s k p l u s p w h
        e r e a i s z e r o b i s o
        n e e t c

        X B E F E G X N E O I K M E
CT:     T E F Y L D Z W L V W I E J
        T F P Y I D O L R P F B A Q
        C S P R C
```

CT: XBEFE GXNEO IKMET EFYLD ZWLVW IEJTF PYIDO LRPFB AQCSP RC.

Chapter 10

ACA Jargon and Familiar Terms

[100/23] - The Ciphertext has 100 letters and 23 different letters are represented.

13-letter sequences - Found in the even decimations of the original alphabet. There are two such sequences for each decimation, and 12 even decimations in all.

A - Aristocrat.

AC - Analyst Corner. A department of *Cm* containing more difficult messages with a "setting" but often no tip.

ACA - American Cryptogram Association.

Alternative transposition block - created by leaving spaces for letters used in the key, so producing a different keyword alphabet.

Anagram - Word or phrase constructed by the transposition of letters from another word, phrase or ciphertext. Anagrams may also be mixed, rather than forming another word.

Aristocrat - Simple substitution cipher with retained word divisions.

Asterisk (*) - (1) Indicates a proper noun in certain ciphers.
(2) Indicates success in solving every cipher in a section of *Cm*.
(3) Indicates unused letters in Xenocrypt plaintext alphabet.
(4) After the number of words in a sudoku indicates the solution appears backwards: Right to left across a row. Bottom to top up a column. Right to left from bottom to top in a 3x3 square.

C - Cryptarithm.

C/A - Used by the intelligence community to mean cryptanalysis.

Cm - Abbreviation for *The Cryptogram*.

CM - Conjugated Matrix. A type of bifid.

Caesar - (noun) Simple substitution cipher, each letter in a crypt being shifted the same amount. (verb) To run each letter in a crypt up or down an alphabet until a word is seen. Aka running down the alphabet.

Chain - An alphabet, or a fragment of an alphabet, created from plaintext and its ciphertext. The chain will be complete when all letters of the alphabet are present in the plaintext.

Challenge - An unusual or difficult problem.

Cipher - A system of secret writing whereby plaintext letters or groups of letters are transformed to hide their meaning. (Not a code)

Cipher alphabet or **ciphertext alphabet** - The alphabet (keyed or normal) which becomes the ciphertext when the plaintext is enciphered. This alphabet is usually written in UPPER CASE LETTERS.

Cipher Exchange - A department of *Cm* containing a variety of cipher types.

Ciphertext - The text produced by applying an encryption method/system to a plaintext message – a cryptogram.

Cleartext - Plaintext.

Code - A special form of substitution cipher in which groups of letters, words, phrases or even whole sentences are replaced by groups of characters chosen arbitrarily.

Completer - A solver who has completed every problem (except specials) in all regular departments of *Cm*; indicated by a * against the name or nom.

Con - A construction; a cipher problem.

Concealment Cipher - Message written in apparent plaintext used to cover hidden message within. See Steganography.

Consonant Line - A cryptanalysis aid in which tentatively identified consonants are graphically displayed.

Contact Count - A cryptanalysis aid, enumeration of different letters contacted by the letter in question.

COPS - Contribution of Postage Stamps. A voluntary donation of stamps or money to help defray costs.

Crib - A clue for entry into a cryptogram. (Also tip)

Cryptanalysis- The steps or processes involved in converting encrypted messages without initial knowledge of the key or the encryption process.

Cryptanalyst - One who solves codes or ciphers without knowledge of the system or keys.

Cryptanalyze - To solve by cryptanalysis.

Cryptarithm - An arithmetic problem in cipher.

Cryptogram - (Crypt); A communication in cipher.

Cryptography - The process of communication encipherment.

Cryptology - The science or study of encryption and decryption.

CS - The “Computer Supplement”; no longer published, but copies are still available.

CT - Ciphertext.

Decimation - The process of constructing a key alphabet from another one by taking letters at a fixed interval starting with the first. The interval must be relatively prime to the length of the alphabet – that is, for a 26-letter alphabet one cannot use an interval of 13 or any even interval, because the resulting alphabet will not include all letters.

Decipher - The specific process the cipher clerk uses to change ciphertext back into plaintext if a cipher is used. To convert ciphertext to plaintext knowing the keys and the system.

Decode - The process the cipher clerk uses to change ciphertext back into plaintext if a code is used.

Decrypt - To convert or transform a cryptogram into the original equivalent plaintext message by a direct reversal of the encrypting process.

Decrypting alphabet - Consists of two rows, the ciphertext letters, written in uppercase, in alphabetical order in the top row and their plaintext equivalents in lowercase in the bottom row. This is a good arrangement for decrypting a simple substitution cipher.

Double hypen (=) - When used in ciphertext indicates that the original plaintext word is hyphenated. A repeated double dash (= =) separates thoughts.

E - The Cipher Exchange.

EB - The Executive Board of the ACA.

Elcy - *Elementary Cryptanalysis*; standard text now entitled *Cryptanalysis* (Dover Books).

Encipher - To convert or transform a plaintext message into a cryptogram by following certain rule, steps, etc. To convert plaintext to ciphertext using a system and a key.

Encrypt - See Encipher.

Encrypting alphabet - Consists of two rows, the plaintext letters, written in lowercase, in alphabetical order in the top row and their ciphertext equivalents in uppercase in the bottom row. This is a good arrangement for encrypting a simple substitution cipher.

Encode - The process the cipher clerk uses to change plaintext to ciphertext if a code is used.

Equivalent alphabet - A mixed alphabet derived from chaining or decimation. Two alphabets are equivalent if they produce the same plaintext or ciphertext. An odd decimation of the original alphabet. There are 12 of these. Example: Headline Puzzles use chaining to find an alphabet equivalent to the original alphabet.

Fractionation - A process whereby a plaintext letter is spread across two or more ciphertext letters. See Bifid and Trifid.

Frequency Chart - Table of number of occurrences of each letter in a text.

Frequency Distribution - Occurrences of letters within the text of any language or ciphertext.

Gadsby - A novel of over 50,000 words written without the use of the letter “e” by Ernest Vincent Wright.

Hyphen (-) - When used in ciphertext this Indicates a word is continued on the next line. This does not indicate proper syllabic hyphenation. (See Double hyphen.)

Index letter -The first letter of the original alphabet.

Index of Coincidence - Likelihood that any pair of letters in a message are equal to each other. Used to determine the key length in a periodic cipher. Also used to decide whether a cryptogram comes from a single alphabet.

K - **Key**.

K1, K2, K3M etc. - Keyword types. (See Chapter 8.)

Kasiski - A method for obtaining the period of a periodic cipher.
(See *Elcy* Chap XIV)

Key - A word, phrase, series of numbers or letters used to control the encipherment process.

Key setting - The letters of the shifted alphabets that stand below the index letter.

Keyed alphabet - A mixed alphabet constructed using a word or phrase. (See Chapter 8.)

Keyword alphabet - Formed by stripping columns from a transposition block, either in left to right sequence or in alphabetical order of the keyword.

Krewe - Members of the ACA.

Mixed alphabet - letters are arbitrarily jumbled or a keyword is used to create the alphabet (see keyed alphabet)

Literal Key - An alphabetic key.

Naturals - An instance where the cipher letter and the plain letter are identical.

Nom - Code name (nom-de-plume) used by some members for anonymity and informality.

Normal alphabet - a b c d e f g h i j k l m n o p q r s t u v w x y z (for English) There are different normal alphabets for other languages.

Null – (1) A letter, without meaning, added to pad out text, break up double letters or provide necessary amount of ciphertext to meet cipher requirements. (2) A type of cipher.

Original alphabet or **original mixed alphabet** - The alphabet for plain letters. The alphabet used to create the ciphertext.

Ornamental - A cipher hidden in a graphic design. (See Steganography.)

P - **Patristocrat**.

Patristocrat - An Aristocrat cipher in 5-letter groups, i.e., word divisions are suppressed.

Pattern Word - A word in which one or more letters are repeated, providing a clue to identity.

Periodics - Ciphers in which substitutions occur in a periodic manner.

Plain alphabet or **plaintext alphabet** - 1) Normal alphabet. 2) The alphabet (keyed or normal) used to determine the plaintext when solving. Usually written in lower case letters when solving or enciphering.

Plaintext - Original message before encipherment (Cleartext).

Polyalphabetic Substitution - A form of cryptography where more than one ciphertext alphabet is used.

Polybius Square - 5 x 5 square used to key substitution ciphers. I/J share one space. 6x6 squares which include 26 letters and 10 digits (See page 27) are used also.

pt - Plaintext.

Public Key Cryptography - System in which messages are encrypted and decrypted by using a combination of keys, one available to the general public and one private.

Quagmire - A mixed alphabet periodic cipher (named for its original keyword).

Scytale - Symbol of the ACA. Ancient Greek cipher device.

Shifted alphabets - The alphabets for cipher letters stand below in the matrix. They may be shifted versions of the original alphabet, or they may be shifted versions of a second alphabet. In all cases these are known as shifted alphabets.

Simple Substitution - A cipher in which each letter of the Plaintext is replaced by one cipher letter, the replacements being unique and no letter standing for itself.

Slidable alphabet - an alphabet that slides against itself.

Slide - A mechanical device for aligning alphabets, used in manual cryptanalysis or encipherment of Periodics.

Sol - A solution.

Special - An unusual or difficult problem.

Steganography - A method of encrypting a message such that the presence of the message is not obvious to the casual observer (for example, Ornamentals, some Grilles, clever Baconians, etc.).

Substitution matrix - In polyalphabetic manual cipher systems a number of alphabets are employed in a substitution matrix. Also used in other than polyalphabetic ciphers, for example in Morbit and Fractionated Morse. This matrix may also be referred to as a tableau.

Tip - A clue for entry into a cryptogram. (crib).

Tramp - A transposition cipher.

Transposition - A cipher retaining the plaintext letters in a re-arranged form.

Transposition block - made by placing a keyword as the first row of the block and then adding the remainder of the alphabet in order in rows below, of the same width as the keyword.

Unknown - A cipher using an unspecified system.

Vigenère - A class of periodic substitution ciphers.

Vowel Line - An analytic aid similar to a Consonant Line.

X - Xenocrypt.

Xenocrypt - A foreign language cipher.

Appendix 1: Morse code

E	·	S	· · ·	H	· · · ·	B	– · · ·	1	· – – – –
T	–	U	· · –	V	· · · –	X	– · · –	2	· · – – –
I	· ·	R	· – ·	F	· · – ·	C	– · – ·	3	· · · – –
A	· –	W	· – –	L	· – · ·	Y	– · – –	4	· · · · –
N	– ·	D	– · ·	P	· – – ·	Z	– – · ·	5	· · · · ·
M	– –	K	– · –	J	· – – –	Q	– – · –	6	– · · · ·
		G	– – ·					7	– – · · ·
		O	– – –					8	– – – · ·
								9	– – – – ·
								0	– – – – –

period (.)	· – · – · –		
comma (,)	– – · · – –	slash (/)	– · · – ·
query (?)	· · – – · ·	equals (=)	– · · · –
colon(:)	– – – · · ·	at (@)	· – – · – ·
semicolon (;)	– · – · – ·	quote (")	· – · · – ·
dash (-)	– · · · · –	apostrophe (')	· – – – – ·

Appendix 2: Vigenère Table

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	pt
Key																											
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	**CT**
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

Appendix 3: Variant Table

Key	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	pt
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
Y	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
X	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
W	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
V	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
U	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
T	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
S	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
R	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
Q	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
P	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
O	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	**CT**
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
L	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
K	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
J	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
I	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
H	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
G	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
F	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
E	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
D	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
C	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
B	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

Appendix 4: Beaufort Table

Key	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	pt
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	
V	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	
U	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	
T	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	
S	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	
R	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	
Q	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	
P	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	
O	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	
N	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	**CT**
M	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	
L	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	
K	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	
J	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	
I	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	
H	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	
G	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	
F	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	
E	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	
D	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	
C	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	
A	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	

Appendix 5: Porta Table

Keys	A	B	C	D	E	F	G	H	I	J	K	L	M
A,B	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C,D	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
E,F	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
G,H	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
I,J	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
K,L	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
M,N	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
O,P	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
Q,R	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
S,T	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
U,V	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
W,X	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
Y,Z	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

Appendix 6: Syllabary Tables

	6	7	1	9	4	3	2	5	Ø	8
8	**A**	**1**	**AL**	**AN**	**AND**	**AR**	**ARE**	**AS**	**AT**	**ATE**
5	**ATI**	**B**	**2**	**BE**	**C**	**3**	**CA**	**CE**	**CO**	**COM**
Ø	**D**	**4**	**DA**	**DE**	**E**	**5**	**EA**	**ED**	**EN**	**ENT**
2	**ER**	**ERE**	**ERS**	**ES**	**EST**	**F**	**6**	**G**	**7**	**H**
4	**8**	**HAS**	**HE**	**I**	**9**	**IN**	**ING**	**ION**	**IS**	**IT**
3	**IVE**	**J**	**Ø**	**K**	**L**	**LA**	**LE**	**M**	**ME**	**N**
1	**ND**	**NE**	**NT**	**O**	**OF**	**ON**	**OR**	**OU**	**P**	**Q**
6	**R**	**RA**	**RE**	**RED**	**RES**	**RI**	**RO**	**S**	**SE**	**SH**
7	**ST**	**STO**	**T**	**TE**	**TED**	**TER**	**TH**	**THE**	**THI**	**THR**
9	**TI**	**TO**	**U**	**V**	**VE**	**W**	**WE**	**X**	**Y**	**Z**

Unknown Coordinates, Known Keysquare
Standard, Unmixed "Alphabet"

	Ø	1	2	3	4	5	6	7	8	9
Ø	**C**	**3**	**H**	**8**	**AR**	**M**	**ING**	**P**	**RI**	**N**
1	**CE**	**A**	**1**	**AL**	**AN**	**AND**	**ARE**	**AS**	**AT**	**ATE**
2	**ATI**	**B**	**2**	**BE**	**CA**	**CO**	**COM**	**D**	**4**	**DA**
3	**DE**	**E**	**5**	**EA**	**ED**	**EN**	**ENT**	**ER**	**ERE**	**ERS**
4	**ES**	**EST**	**F**	**6**	**G**	**7**	**HAS**	**HE**	**I**	**9**
5	**IN**	**ION**	**IS**	**IT**	**IVE**	**J**	**Ø**	**K**	**L**	**LA**
6	**LE**	**ME**	**ND**	**NE**	**NT**	**O**	**OF**	**ON**	**OR**	**OU**
7	**Q**	**R**	**RA**	**RE**	**RED**	**RES**	**RO**	**S**	**SE**	**SH**
8	**ST**	**STO**	**T**	**TE**	**TED**	**TER**	**TH**	**THE**	**THI**	**THR**
9	**TI**	**TO**	**U**	**V**	**VE**	**W**	**WE**	**X**	**Y**	**Z**

Known Coordinates, Unknown Keysquare
0-9, Keyword-mixed Keysquare

	6	7	1	9	4	3	2	5	0	8
8	**C**	**3**	**H**	**8**	**AR**	**M**	**ING**	**P**	**RI**	**N**
5	**CE**	**A**	**1**	**AL**	**AN**	**AND**	**ARE**	**AS**	**AT**	**ATE**
0	**ATI**	**B**	**2**	**BE**	**CA**	**CO**	**COM**	**D**	**4**	**DA**
2	**DE**	**E**	**5**	**EA**	**ED**	**EN**	**ENT**	**ER**	**ERE**	**ERS**
3	**ES**	**EST**	**F**	**6**	**G**	**7**	**HAS**	**HE**	**I**	**9**
4	**IN**	**ION**	**IS**	**IT**	**IVE**	**J**	**Ø**	**K**	**L**	**LA**
1	**LE**	**ME**	**ND**	**NE**	**NT**	**O**	**OF**	**ON**	**OR**	**OU**
6	**Q**	**R**	**RA**	**RE**	**RED**	**RES**	**RO**	**S**	**SE**	**SH**
7	**ST**	**STO**	**T**	**TE**	**TED**	**TER**	**TH**	**THE**	**THI**	**THR**
9	**TI**	**TO**	**U**	**V**	**VE**	**W**	**WE**	**X**	**Y**	**Z**

Unknown coordinates, Unknown Keysquare

Appendix 7: Xenocrypt Syllabary Tables

French Syllabary Square

	0	1	2	3	4	5	6	7	8	9
0	**A**	**1**	**AI**	**AIS**	**AIT**	**AN**	**ANS**	**AR**	**AS**	**B**
1	**2**	**C**	**3**	**CE**	**D**	**4**	**DAN**	**DE**	**DEL**	**DES**
2	**DU**	**E**	**5**	**ED**	**EDE**	**EL**	**ELL**	**EM**	**EME**	**EN**
3	**ENT**	**ER**	**ES**	**ESE**	**EST**	**EUR**	**F**	**6**	**G**	**7**
4	**GE**	**H**	**8**	**I**	**9**	**IE**	**ION**	**IT**	**J**	**Ø**
5	**K**	**L**	**LA**	**LE**	**LES**	**LLE**	**M**	**ME**	**MEN**	**N**
6	**NE**	**NO**	**NON**	**NS**	**NT**	**O**	**ON**	**ONT**	**OU**	**OUI**
7	**OUR**	**OUS**	**P**	**PAR**	**Q**	**QU**	**QUE**	**QUI**	**R**	**RE**
8	**RES**	**S**	**SE**	**SSE**	**T**	**TE**	**TI**	**TIO**	**TRE**	**TTE**
9	**U**	**UI**	**UN**	**UNE**	**UR**	**V**	**W**	**X**	**Y**	**Z**

German Syllabary Square

	0	1	2	3	4	5	6	7	8	9
0	**A**	**1**	**AB**	**AHT**	**ALS**	**AM**	**AN**	**AU**	**AUF**	**B**
1	**2**	**BE**	**BEN**	**BER**	**C**	**3**	**CH**	**CHE**	**CHT**	**D**
2	**4**	**DA**	**DE**	**DEN**	**DER**	**DES**	**DI**	**DIE**	**DU**	**E**
3	**5**	**EI**	**EIN**	**EL**	**EN**	**END**	**ER**	**F**	**6**	**G**
4	**7**	**GE**	**GEN**	**H**	**8**	**HA**	**HE**	**HEN**	**I**	**9**
5	**ICH**	**IE**	**IN**	**ISC**	**IST**	**IT**	**J**	**Ø**	**K**	**L**
6	**M**	**MI**	**MIT**	**N**	**ND**	**NDE**	**NE**	**NO**	**NS**	**NUR**
7	**O**	**OB**	**P**	**Q**	**R**	**RCH**	**RE**	**S**	**SCH**	**SE**
8	**ST**	**T**	**TE**	**TEN**	**U**	**UE**	**UM**	**UN**	**UND**	**UNG**
9	**V**	**VON**	**W**	**WAR**	**WAS**	**WO**	**X**	**Y**	**Z**	**ZU**

Italian Syllabary Square

	0	1	2	3	4	5	6	7	8	9
0	**A**	**1**	**AL**	**AN**	**AR**	**ATO**	**B**	**2**	**C**	**3**
1	**CA**	**CHE**	**CI**	**CO**	**D**	**4**	**DA**	**DE**	**DI**	**E**
2	**5**	**EL**	**EN**	**ER**	**ES**	**ET**	**F**	**6**	**G**	**7**
3	**GI**	**H**	**8**	**I**	**9**	**IA**	**IC**	**IL**	**IN**	**ION**
4	**IS**	**IT**	**J**	**Ø**	**K**	**L**	**LA**	**LE**	**LI**	**LL**
5	**LO**	**M**	**MA**	**ME**	**MI**	**MO**	**N**	**NA**	**NE**	**NI**
6	**NO**	**NTE**	**O**	**OL**	**ON**	**OR**	**OS**	**P**	**PA**	**PER**
7	**PO**	**PR**	**Q**	**R**	**RA**	**RE**	**RI**	**RO**	**S**	**SA**
8	**SE**	**SI**	**SO**	**SS**	**ST**	**T**	**TA**	**TE**	**TI**	**TO**
9	**TR**	**TT**	**U**	**UN**	**V**	**W**	**X**	**Y**	**Z**	**ZIO**

Latin Syllabary Square

	0	1	2	3	4	5	6	7	8	9
0	**A**	**1**	**AD**	**AE**	**AM**	**ANT**	**AS**	**AT**	**ATI**	**ATU**
1	**B**	**2**	**BUS**	**C**	**3**	**CON**	**CUM**	**D**	**4**	**E**
2	**5**	**EM**	**ENT**	**EQU**	**ER**	**ERA**	**ERI**	**ES**	**ET**	**EX**
3	**F**	**6**	**G**	**7**	**H**	**8**	**I**	**9**	**IA**	**IBU**
4	**IN**	**IO**	**ION**	**IS**	**ISS**	**IT**	**ITA**	**ITU**	**J**	**Ø**
5	**K**	**L**	**M**	**N**	**NE**	**NT**	**O**	**OS**	**P**	**PER**
6	**PRO**	**Q**	**QUA**	**QUE**	**QUI**	**QUO**	**R**	**RA**	**RAT**	**RE**
7	**RI**	**RUM**	**S**	**SE**	**SI**	**SSE**	**STR**	**T**	**TA**	**TAT**
8	**TE**	**TER**	**TI**	**TIS**	**TO**	**TUM**	**TUR**	**U**	**UA**	**UI**
9	**UM**	**UNT**	**UR**	**US**	**UT**	**V**	**W**	**X**	**Y**	**Z**

Spanish Syllabary Square

	0	1	2	3	4	5	6	7	8	9
0	**A**	**1**	**AD**	**ADO**	**AL**	**AQU**	**AR**	**ARA**	**AS**	**B**
1	**2**	**C**	**3**	**CI**	**CIO**	**CO**	**CON**	**D**	**4**	**DE**
2	**DEL**	**DI**	**E**	**5**	**EDE**	**EL**	**EN**	**ER**	**ES**	**EST**
3	**F**	**6**	**G**	**7**	**H**	**8**	**HAY**	**I**	**9**	**IO**
4	**IST**	**J**	**Ø**	**K**	**L**	**LA**	**LAS**	**LO**	**LOS**	**M**
5	**MAS**	**ME**	**MI**	**MUY**	**N**	**NEI**	**NO**	**NON**	**NTE**	**O**
6	**ON**	**OR**	**OS**	**OSA**	**P**	**PER**	**POR**	**Q**	**QU**	**QUE**
7	**R**	**RA**	**RE**	**RES**	**S**	**SDE**	**SE**	**SER**	**SI**	**SIN**
8	**SON**	**SI**	**SU**	**SUS**	**T**	**TA**	**TE**	**TI**	**TU**	**U**
9	**UE**	**UN**	**UNA**	**UNO**	**V**	**VA**	**W**	**X**	**Y**	**Z**

WHO WILL GET YOUR CRYPTOGRAPHIC TREASURES WHEN YOU DIE?

By B. NATURAL

It is rare that more than one member of a family is a cryptographer. During his lifetime that member collects certain cryptographic files, books, references, word-lists, and the like, all of which are of only sentimental value to the rest of his family, but which are of inestimable value to someone else in the Krewe.

All too often when a cryptographer dies, his treasures fall into the hands of unappreciative persons and are either wasted or destroyed instead of being sold or given to those who could use them to advantage.

In one instance in the past, a splendid library of cryptographic “finds” had been left, but it was impossible to induce the widow to part with a single item. In another case a member left his library to his sister who was non-cryptographic, and the articles were rescued from an outhouse where they were piled helter-skelter, a prey to mice and dampness and black with dust and grime.

In view of such cases, a suggestion seems to be in order. All members of the ACA who have accumulated files, books, and other items of value to other cryptographers, should leave them in some written directions in their wills, as to what should become of these materials.

Don’t let these priceless books and files be sold for waste paper or used to start the furnace fires in a non-cryptographic household. See that they are passed on either by sale or gift, to other members of the Krewe, by whom they will be appreciated and used exactly as they should be.